IP Address	http://192.168.10.1
Password	1234

Firmware Version 1.53
Edition 1, 7/2011

MWR222

Mobile Wireless Router

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the MWR222 using the Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Supporting Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.us.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

SUPPORT E-MAIL	WEB SITE
techwriter@zyxel.com	www.zyxel.com

Customer Support

Please have the following information ready when you contact Customer Support:

- Product model and serial number
- Warranty information
- Date that you received or purchased your device
- Brief description of the problem including any steps that you have taken before contacting the ZyXEL Customer Support representative

Support Email	support@zyxel.com
Toll-Free	1-800-978-7222
Website	www.us.zyxel.com
Postal mail	ZyXEL Communications Inc. 1130 N. Miller Street, Anaheim, CA 92806-2001 U.S.A.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide:

> **Warnings tell you about things that could harm you or your device.**

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The MWR222 may be referred to as the "MWR222", the "device", the "product" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text. For example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** submenu, and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g." is a shorthand for "for instance" and "i.e." means "that is" or "in other words."

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The MWR222 icon is not an exact representation of your device.

MWR222	Computer	Notebook computer
Server	Modem	Firewall
Telephone	Switch	Router

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do not leave the device exposed to a heat source or in a high-temperature location such as in the sun or in an unattended vehicle. To prevent damage, remove the device from the vehicle or store it out of direct sunlight
- When storing the device for an extended time, store within the following temperature range: from 32° to 77°F
- Do NOT operate the device in temperatures colder than 32° or hotter than 104° F
- Contact your local waste disposal department to dispose of the device/battery in accordance with applicable local laws and regulations.
- Do NOT expose your device to dampness, dust, or corrosive liquids.
- Do NOT keep the unit power on while putting it into suite case, closed box, luggage, computer bag and any closed storage, do turn the device power off before storage.
- Do NOT place items on top of the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Connect cables only to their corresponding ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY the power adaptor or cord provided by the manufacturer for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can step on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Before inserting a USB device or accessory. Please verify power consumption of the device is within the the standard USB 2.0 power rating range of 500 mA per port.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device's ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- Use ONLY USB devices listed on the manufacturer's website (http://us.zyxel.com/mwr).

Battery Warnings

Please follow the safety guidelines described in the safety warning and battery warning. Failing to do so may shorten the lifespan of the internal lithium ion battery or may present a risk of damage to the unit, fire, chemical burn, electrolyte leak and/or injury.

- Do not leave unit exposed to a heat source or in a location that may become hot, such as a parked vehicle or in direct sunlight. Do not leave in a glove box, trunk or other location that may become hot.
- Do not puncture or incinerate the device or battery.
- When/if you dispose of the battery, be certain to follow ordinances from local waste disposal agencies.
- Keep the battery away from small children or pets.
- Never use a knife, screwdriver or other sharp object to remove the battery.
- Do not attempt to open the battery.
- Use only the provided recharger to recharge the battery.
- Only replace the battery with the correct replacement battery. Failure to do so may result in fire or explosion. Contact ZyXEL to obtain the correct replacement battery.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Part I: Introduction 17

Chapter 1
Getting to Know Your MWR222 18

1.1 Overview 18
1.2 Applications 18
1.3 Ways to Manage the MWR222 19
1.4 Good Habits for Managing the MWR222 20
1.5 LEDs 20

Chapter 2
Introducing the Web Configurator 22

2.1 Overview 22
2.2 Accessing the Web Configurator 22
2.2.1 Login Screen 23
2.2.2 Password Screen 23
2.3 Resetting the MWR222 24
2.3.1 Procedure to Use the Reset Button 24

Chapter 3
Monitor 25

3.1 Overview 25
3.2 What You Can Do 25
3.3 BW MGMT Monitor 25
3.4 DHCP Table 26
3.5 Packet Statistics 27
3.6 WLAN Station Status 29
3.7 MWAN MGMT Monitor 29

Chapter 4
MWR222 Modes 32

4.1 Overview 32
4.1.1 Device Modes 32

Chapter 5
Router Mode 34

5.1 Overview 34
5.2 What You Can Do 34
5.3 Status Screen 35
5.3.1 Navigation Panel 40

Chapter 6
Access Point Mode 45

6.1 Overview 45
6.2 What You Can Do 45
6.3 What You Need to Know 46
6.3.1 Setting your MWR222 to AP Mode 46
6.3.2 Accessing the Web Configurator in Access Point Mode 47
6.3.3 Configuring your WLAN, Bandwidth Management and Maintenance Settings 47
6.4 AP Mode Status Screen 48
6.4.1 Navigation Panel 51
6.5 LAN Screen 51

Chapter 7
WISP Mode 54

7.1 Overview 54
7.2 What You Can Do 55
7.3 What You Need to Know 55
7.3.1 Setting your MWR222 to WISP Mode 55
7.3.2 Accessing the Web Configurator in WISP Mode 56
7.4 WISP Mode Status Screen 57
7.5 Wireless LAN General Screen 60
7.5.1 No Security 61
7.5.2 Static WEP 62
7.5.3 WPA(2)-PSK 64
7.5.4 Advance Screen 65
7.5.5 Site Survey 66

Chapter 8
Tutorials 69

8.1 Overview 69
8.2 Connecting to the Internet 69
8.2.1 DSL Modem 69
8.2.2 Cable Modem 70
8.2.4 3G USB Adapter 70
8.3 Connecting to the Internet from an Access Point 71
8.4 Configuring Wireless Security Using WPS 72
8.4.1 Push Button Configuration (PBC) 72
8.4.2 PIN Configuration 73
8.5 Enabling and Configuring Wireless Security (No WPS) 74
8.5.1 Configure Your Notebook 76

Part II: Network 79

Chapter 9
Wireless LAN 80

9.1 Overview 80
9.2 What You Can Do 81
9.3 What You Should Know 81
9.3.1 Wireless Security Overview 81
9.4 General Wireless LAN Screen 84
9.5 Security 85
9.5.1 No Security 85
9.5.2 WEP Encryption 86
9.5.3 WPA-PSK/WPA2-PSK 88
9.6 MAC Filter 90
9.7 Wireless LAN Advanced Screen 91
9.8 Quality of Service (QoS) Screen 93
9.9 WPS Screen 94
9.10 WPS Station Screen 96
9.11 Scheduling Screen 97
9.12 WDS Screen 98

Chapter 10
WAN 100

10.1 Overview 100
10.2 What You Can Do 101
10.3 What You Need To Know 101
10.3.1 Configuring Your Internet Connection 101
10.3.2 Multicast 102
10.4 Internet Connection 103

10.4.1 Ethernet Encapsulation 103
10.4.2 PPPoE Encapsulation 106
10.4.3 PPTP Encapsulation 109
10.4.4 L2TP Encapsulation 113
10.5 Mobile WAN 117
10.6 Advanced WAN Screen 126
10.7 IGMP Snooping Screen 127

Chapter 11
LAN 128

11.1 Overview 128
11.2 What You Can Do 128
11.3 What You Need To Know 128
11.3.1 IP Pool Setup 129
11.3.2 LAN TCP/IP 129
11.3.3 IP Alias 129
11.4 LAN IP Screen 129
11.5 IP Alias Screen 130

Chapter 12
DHCP Server 132

12.1 Overview 132
12.2 What You Can Do 132
12.3 General Screen 132
12.4 Advanced Screen 133

Chapter 13
Network Address Translation (NAT) 136

13.1 Overview 136
13.2 What You Can Do 136
13.3 General NAT Screen 137
13.4 NAT Application Screen 138
13.5 NAT Advanced Screen 140
13.5.1 Trigger Port Forwarding Example 142
13.5.2 Two Points To Remember About Trigger Ports 143

Chapter 14
Dynamic DNS 144

14.1 Overview 144
14.2 What You Can Do 144
14.3 What You Need To Know 144
14.4 Dynamic DNS Screen 144

Chapter 15
OpenDNS 146

15.1 Overview 146
15.2 What You Can Do 146
15.3 OpenDNS Screen 146

Chapter 16
Static Route 148

16.1 Overview 148
16.2 What You Can Do 148
16.3 IP Static Route Screen 148

Chapter 17
RIP 151

17.1 Overview 151
17.2 What You Can Do 151
17.3 RIP Screen 151

Part III: Security 153

Chapter 18
Firewall 154

18.1 Overview 154
18.2 What You Can Do 154
18.3 What You Need To Know 155
18.4 General Firewall Screen 155
18.5 Services Screen 156

Chapter 19
Content Filter 160

19.1 Overview 160
19.2 What You Can Do 160
19.3 What You Need To Know 160
19.3.1 Content Filtering Profiles 160
19.4 Content Filter Screen 161

Part IV: Management 164

Chapter 20
Bandwidth Management 165

20.1 Overview 165

20.2 What You Can Do 165
20.3 What You Need To Know 166
20.4 General Screen 166
20.5 Advanced Screen 167
20.5.1 Rule Configuration: Application Rule Configuration 170
20.5.2 Rule Configuration: User Defined Service Rule Configuration 171
20.6 Monitor Screen 173
20.6.1 Predefined Bandwidth Management Services 173

Chapter 21
Remote Management 175

21.1 Overview 175
21.2 What You Can Do 175
21.3 What You Need to Know 175
21.3.1 Remote Management and NAT 176
21.3.2 System Timeout 176
21.4 WWW Screen 176
21.5 SNMP Screen 177

Chapter 22
Universal Plug-and-Play (UPnP) 178

22.1 Overview 178
22.2 What You Can Do 178
22.3 What You Need to Know 178
22.3.1 NAT Traversal 178
22.3.2 Cautions with UPnP 179
22.4 UPnP Screen 179
22.5 Technical Reference 180
22.5.1 Using UPnP in Windows XP Example 180
22.5.2 Web Configurator Easy Access 183

Part V: Maintenance and Troubleshooting 186

Chapter 23
Maintenance 187

23.1 Overview 187
23.2 What You Can Do 187
23.3 General Screen 187

Chapter 24
Password 189

24.1 Overview 189
24.2 What You Can Do 189
24.3 What You Need to Know 189
24.4 Password Screen 189

Chapter 25
Time 191

25.1 Overview 191
25.2 What You Can Do 191
25.3 Time Setting Screen 191

Chapter 26
Firmware Upgrade 194

26.1 Overview 194
26.2 What You Can Do 194
26.3 Firmware Upload Screen 194

Chapter 27
Backup/Restore 196

27.1 Overview 196
27.2 What You Can Do 196
27.3 Configuration Screen 196

Chapter 28
Reset/Restart 199

28.1 Overview 199
28.2 What You Can Do 199
28.3 Reset/Restart Screen 199

Chapter 29
Sys OP Mode 200

29.1 Overview 200
29.2 What You Can Do 200
29.3 What You Need to Know 200
29.4 Sys Op Mode Screen 202

Chapter 30
Alert 204

30.1 Overview 204
30.2 What You Can Do 204
30.3 Alert Screen 204

Chapter 31
Troubleshooting 207

31.1 Power, Hardware Connections, and LEDs 207
31.2 MWR222 Access and Login 208
31.3 Internet Access 210
31.4 Resetting the MWR222 to Its Factory Defaults 211
31.5 Wireless Router/AP Troubleshooting 212

Chapter 32
Product Specifications 218

Part VI: Appendices and Index 222

Appendix A Pop-up Windows, JavaScripts and Java Permissions 223

Appendix B IP Addresses and Subnetting 231

Appendix C Setting up Your Computer's IP Address 244

Appendix D Wireless LANs 263

Appendix E Common Services 276

Appendix F Legal Information 281

Appendix G Open Source Licenses 285

Part I: Introduction

Getting to Know Your MWR222

Introducing the Web Configurator

Monitor

MWR222 Modes

Tutorials

1. Getting to Know Your MWR222

1.1 Overview

This chapter introduces the main features and applications of the MWR222.

Like a high performance wireless router, the MWR222 extends the range of your existing wired network without additional wiring, providing easy network access to in-home and in-office users. It also features two USB ports - One on the back, to connect to a compatible 3G modem when the land line is down or simply not available, and one on the side which is reserved for future expansion. The 3G connection allows you to connect to the Internet anywhere you have wireless 3G coverage from your mobile broadband provider. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

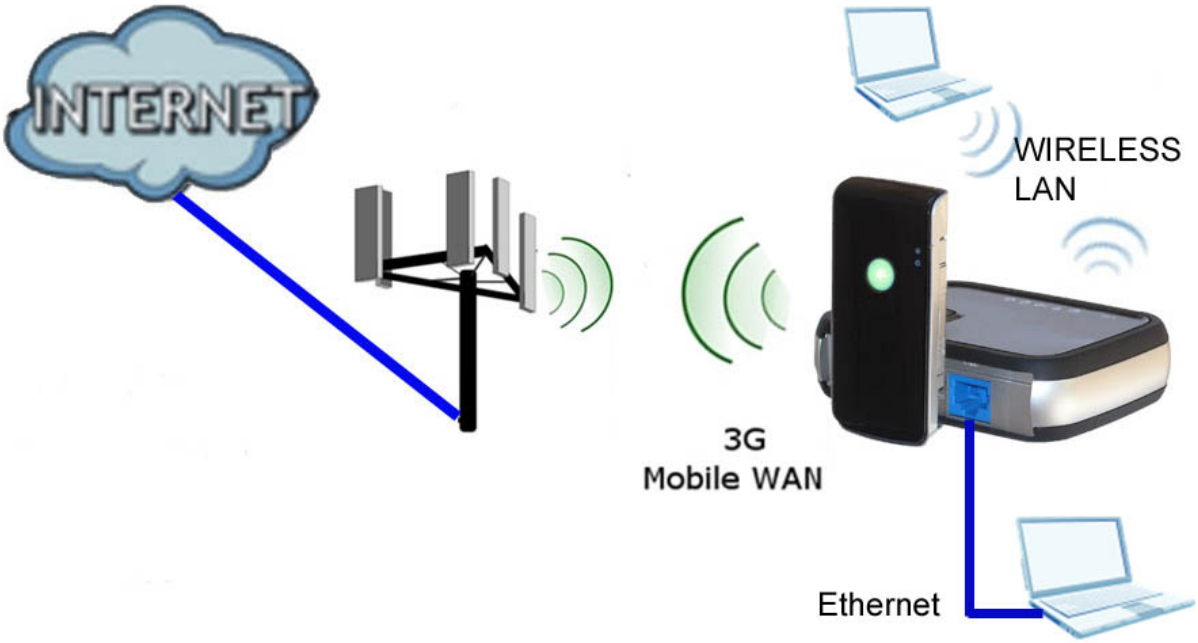
A range of services such as a firewall and content filtering are also available for secure Internet computing. You can use media bandwidth management to efficiently manage traffic on your network. Bandwidth management features allow you to prioritize time-sensitive or highly important applications such as Voice over Internet Protocol (VoIP).

1.2 Applications

You can create the following networks using the MWR222:

- **Wired**. You can connect a network device via the Ethernet port of the MWR222 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the MWR222 to access network resources.
- **Land line / Wireless WAN**. Connect to a broadband modem/router for Internet access or connect to Internet via 3G data service.
- **Internet access** for small business groups in areas where cable modem, DSL or even T-1 connections are not available.

Figure 1 MWR222 Network



1.3 Ways to Manage the MWR222

Use any of the following methods to manage the MWR222.

- Web Configurator. This is recommended for everyday management of the MWR222 using a (supported) web browser.
- SNMP management. This allows you to manage your MWR222 with a group of networked devices from a management program. Currently MWR222 supports SNMP v1, with further support available for future releases.
- Wireless switch. You can use the built-in switch of the MWR222 to turn the wireless function on and off without opening the Web Configurator.
- WPS (Wi-Fi Protected Setup) button. You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL device.

1.4 Good Habits for Managing the MWR222

Do the following things regularly to make the MWR222 more secure and to manage the MWR222 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the MWR222 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the MWR222. You could simply restore your last configuration.

1.5 LEDs

Figure 2 Front Panel

The following table describes the LEDs and the WPS button.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The MWR222 is receiving power and functioning properly.
		Slow Blinking	The MWR222 is booting.
		Fast Blinking	The reset button has been pressed longer than 5 seconds and the MWR222 is being reset to factory default configuration.
		Off	The MWR222 is not receiving power.
Battery	Green	On	The MWR222 is charged.
	Amber	On	The MWR222 is charging.
	Red	On	The MWR222 is low on battery power.
		Blinking	The MWR222 is VERY LOW on battery power. If AC power is not supplied within 10 minutes, the MWR222 will automatically shut down.

WLAN	Green	On	The MWR222 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The MWR222 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS	Green	On	WPS is enabled.
		Blinking	The MWR222 is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.

LAN 1	Green	On	The MWR222 has a successful 10/100MB Ethernet connection.
		Blinking	The MWR222 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
USB	Green	On	The 3G connection has been established.
		Blinking Slowly	The 3G connection has established and is in STANDBY mode.
		Blinking Quickly	The 3G connection is establishing, or there has been an error in connecting to the 3G connection.
		Off	The 3G adapter is disconnected, or the 3G adapter could not be recognized by the MWR222.

2. Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the MWR222 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the MWR222 via Internet browser. Use Internet Explorer 7.0 and later or Firefox 3.0 and later versions or Safari 4.0 or later versions. The recommended screen resolution is 1024 by 768 pixels or higher. In order to use the Web Configurator you need to allow:

• Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
• JavaScripts (enabled by default).
• Java permissions (enabled by default).
Refer to the Troubleshooting chapter (Chapter 32) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1 Make sure your MWR222 hardware is properly connected and prepare your computer or computer network to connect to the MWR222 (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "http://192.168.10.1" as the website address. Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 3 Login screen

ZyXEL
MWR-222
Welcome to the router configuration interface. Enter the password and click 'Login'.
Password :
Login
(max. 30 alphanumeric, printable characters and no spaces)

The following table describes the labels in this screen.

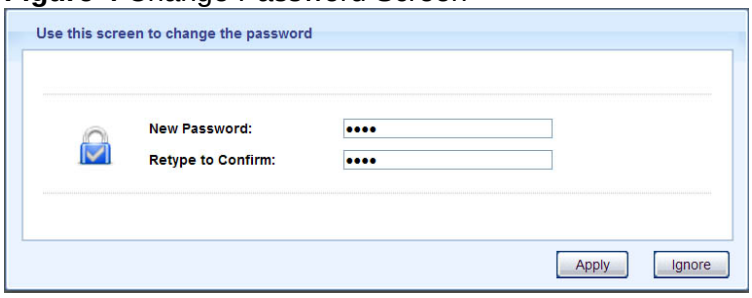
Table 2 Login screen

LABEL	DESCRIPTION
Password	Type “1234” (default) as the password.

2.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 4 Change Password Screen



The following table describes the labels in this screen.

Table 3 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to	Retype the password for confirmation.

Confirm

Apply	Click **Apply** to save your changes to the MWR222.
Ignore	Click **Ignore** if you do not want to change the password at this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 24 to see how to change this). Simply log back into the MWR222 if this happens.

2.3 Resetting the MWR222

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the MWR222 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234," and the IP address will be reset to "192.168.10.1".

2.3.1 Procedure to Use the Reset Button

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than one second to restart/reboot the MWR222.

3 Press the **RESET** button for longer than five seconds to set the MWR222 back to its factory-default configurations. The Power LED will start to blink to indicate that the default configuration is being loaded.

3. Monitor

3.1 Overview

This chapter discusses read-only information related to the device state of the MWR222.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Status screen to view the bandwidth consumed, packets sent/received as well as the status of clients connected to the MWR222.

3.2 What You Can Do

- Use the **BW MGMT Monitor** screen to view the amount of network bandwidth that applications running in the network are using. (future release)
- Use the **DHCP Table** screen to view information related to your DHCP status.
- Use the **Packet Statistics** screen to view port status, packet specific statistics, system uptime, and so on.
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the MWR222.

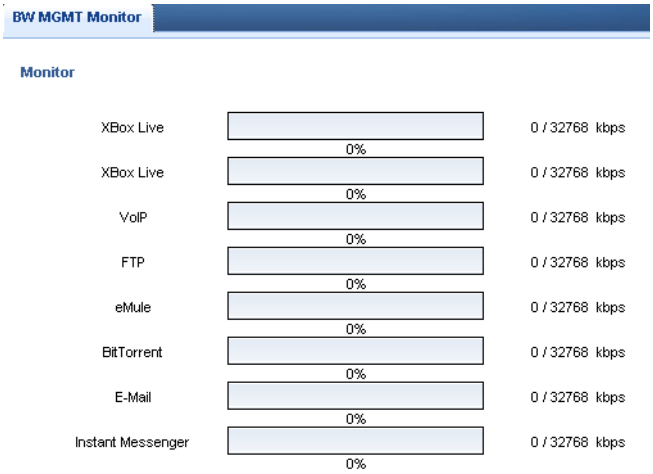
3.3 BW MGMT Monitor

The Bandwidth Management (BW MGMT) Monitor allows you to view the amount of network bandwidth that applications running in the network are using.

Bandwidth is measured in kilobits per second (kbps).

The monitor shows what kinds of applications are running in the network, the maximum kbps that each application can use, as well as the percentage of bandwidth each application is currently using.

Figure 5 Summary: BW MGMT Monitor



3.4 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the MWR222's LAN as a DHCP server or disable it. When configured as a server, the MWR222 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network. Otherwise, the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen. Information displayed here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the MWR222's DHCP server.

Figure 6 Summary: DHCP Table

The following table describes the labels in this screen.

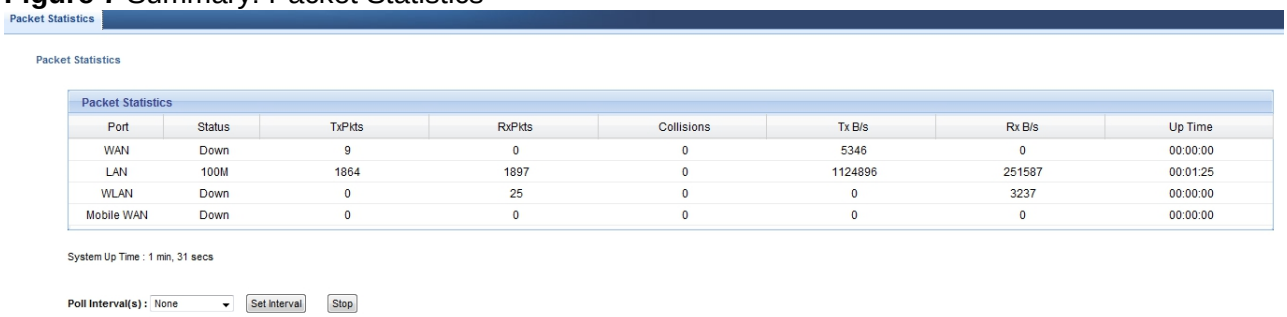
Table 4 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
IP Address	This field displays the IP address relative to the # field listed above.
Expires in	This field displays the time when the IP address and MAC address association ends.
Refresh	Click **Refresh** to renew the screen.

3.5 Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Information displayed here includes port status, packet specific statistics and system uptime. The **Poll Interval(s)** field allows you to configure the rate at which the Packet Statistics screen is refreshed.

Figure 7 Summary: Packet Statistics


Packet Statistics
Packet Statistics
Packet Statistics
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
WAN Down 9 0 0 5346 0 00:00:00
LAN 100M 1864 1897 0 1124896 251587 00:01:25
WLAN Down 0 25 0 0 3237 00:00:00
Mobile WAN Down 0 0 0 0 0 00:00:00
System Up Time : 1 min, 31 secs
Poll Interval(s) : None
Set Interval
Stop

The following table describes the labels in this screen.

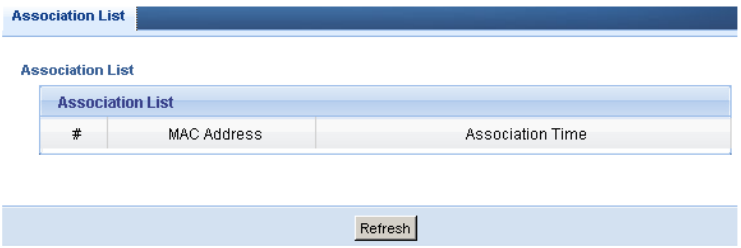
Table 5 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	Displays the MWR222's port type.
Status	The LAN Port field displays the port speed and duplex setting if the device is currently connected, or **Down** if the device is disconnected. The WAN Port field displays the port speed and duplex setting if you're using Ethernet encapsulation. If you're using PPoE or PPTP encapsulation, it will display **Idle** if the line is idle, **Dial** if the device is starting to trigger a call, or **Drop** if the device is dropping a call. This field displays **Down** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	Displays the number of transmitted packets on this port.
RxPkts	Displays the number of received packets on this port.
Collisions	Displays the number of collisions on this port.
Tx B/s	Displays the transmission speed in bytes per second on this port.
Rx B/s	Displays the reception speed in bytes per second on this port.
Up Time	Displays the length of time the MWR222 has been during this session.
System Up Time	Displays the total time the MWR222 has been on during all sessions.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

3.6 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. The **Association List** displays the wireless stations that are currently associated with the MWR222. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 8 Summary: Wireless Association List



The following table describes the labels in this screen.

Table 6 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the MWR222's WLAN network.
Refresh	Click **Refresh** to reload the list.

3.7 MWAN MGMT Monitor

Click the **MWAM MGMT Monitor (Details...)** hyperlink in the **Status** screen. View the connection details of the Mobile WAN and information about the 3G USB adapter.

Figure 9 Summary: Mobile WAN Connection Information

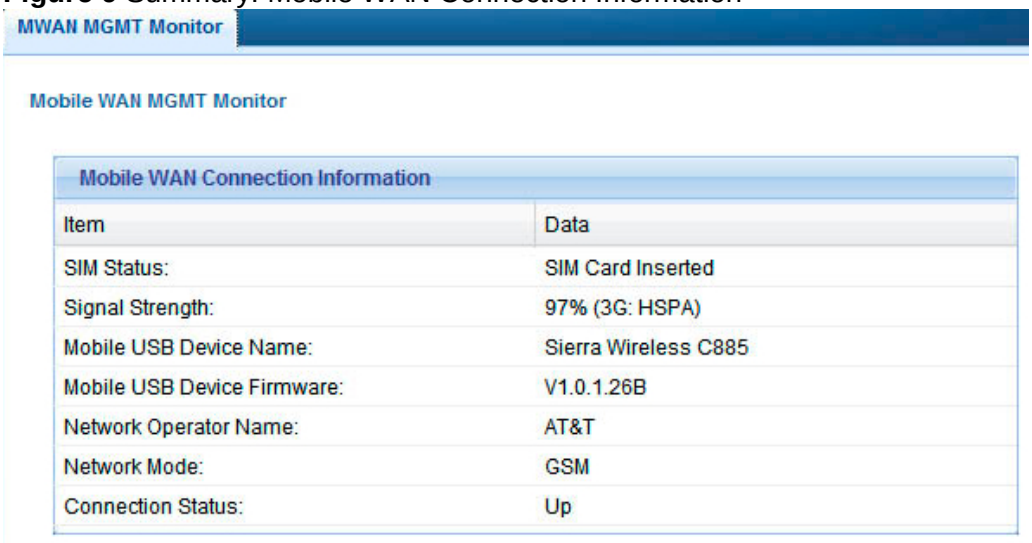


Figure 10 Summary: LTE/3G Mobile WAN Connection Information

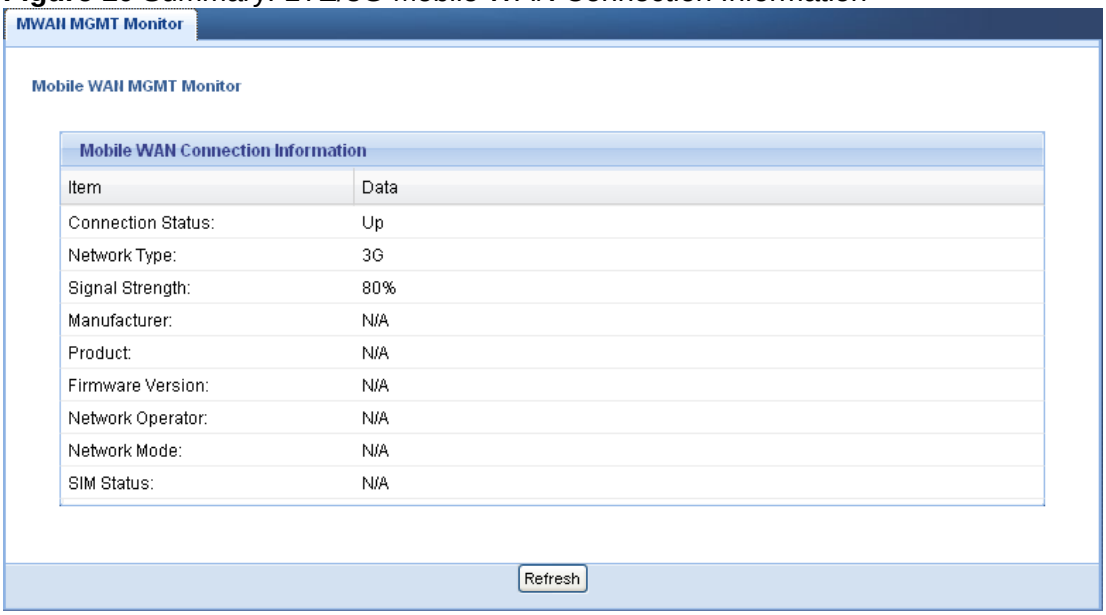
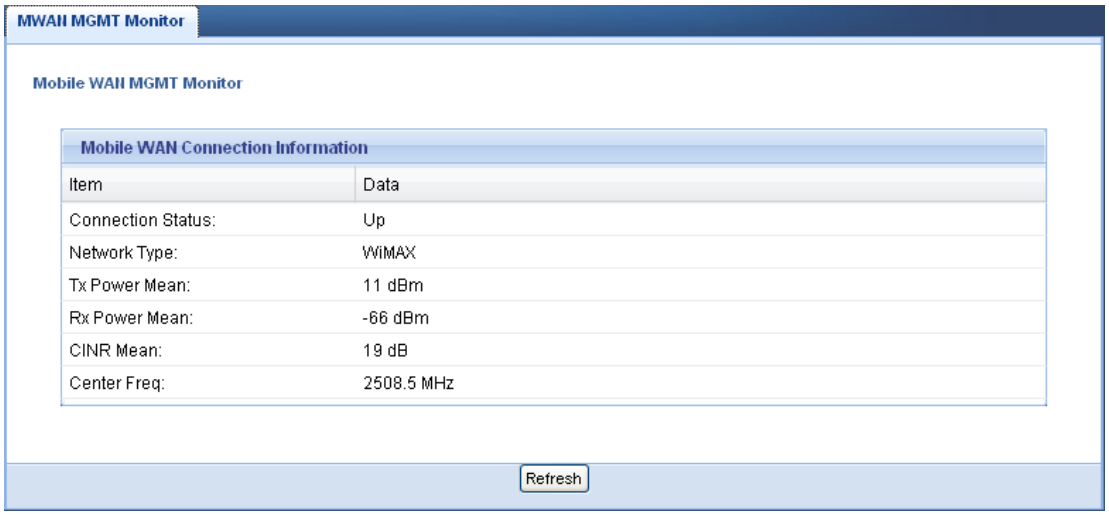


Table 7 Summary: Mobile WAN Connection Information

LABEL	DESCRIPTION
Connection Status	This field displays the status of your 3G connection.
Network Type	This field displays the type of your network.
Signal Strength	This field displays the signal strength of your 3G connection.
Manufacturer	This field displays the manufacturer of your mobile USB device.

Product	This field displays the product name of your mobile USB device.
Firmware Version	This displays the firmware version of your mobile USB device.
Network Operater	This field displays the name of your mobile ISP.
Network Mode	This displays the current network mode of your 3G connection.
SIM status	This field displays the status of your SIM card.

Figure 11 Summary: WiMAX Mobile WAN Connection Information



The following table describes the labels in this screen.

Table 8 Summary: Mobile WAN Connection Information

LABEL	DESCRIPTION
Connection Status	This field displays the status of your connection.
Network Type	This field displays the current network type of your mobile connection.
Tx Power Mean	This field displays the average transmitting power of your WiMAX connection.

Rx Power Mean	This field displays the average receiving power of your WiMAX connection.
CINR Mean	This displays the average CINR of your WiMAX connection
Center Freq.	This displays the center frequency of your WiMAX connection.

4. MWR222 Modes

4.1 Overview

This chapter introduces the different modes available on your MWR222.

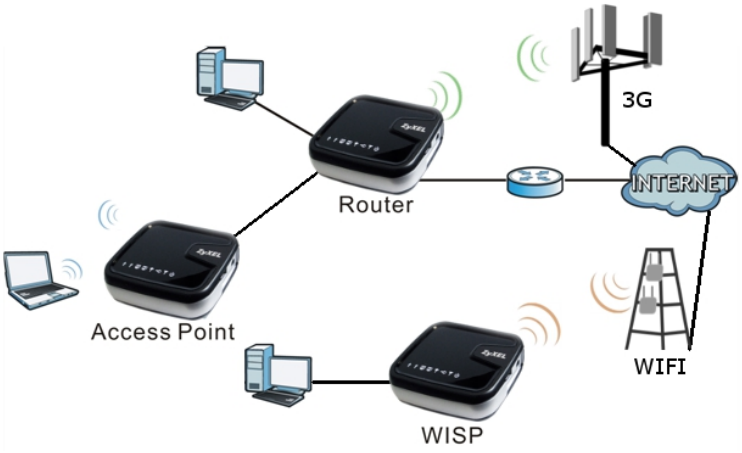
4.1.1 Device Modes

This refers to the operating mode of the MWR222, which can act as a:

- **Router**. This is the default device mode of the MWR222. Use this mode to connect the local network to another network, like the Internet. Go to Status Screen to view the **Status** screen in this mode.
- **Access Point**. Use this mode if you want to extend your network by allowing network devices to connect to the MWR222 wirelessly. Go to AP Mode to view the **Status** screen in this mode.
- **WISP** mode. Use this mode if there is an existing access point in the network to which you want to connect your local network. Go to WISP Mode S to view the **Status** screen in this mode.

The following figure is a simple illustration of the device configuration modes of the MWR222.

Figure 12 Device Mode Example



For more information on these modes and to change the mode of your MWR222, refer to Chapter 30.

Note: Choose your Device Mode carefully to avoid having to change it later.

When changing to another mode, the IP address of the MWR222 changes. The running applications and services of the network devices connected to the MWR222 can be interrupted.

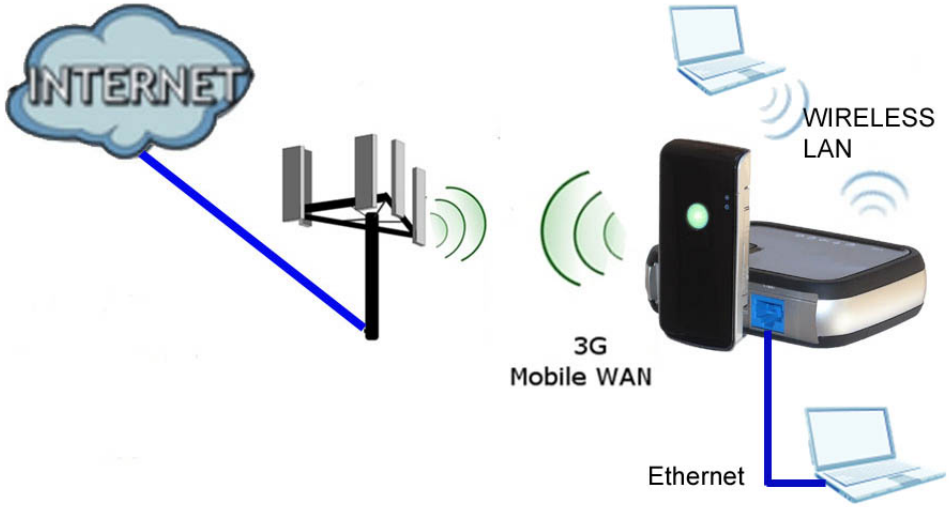
In WISP mode, you should know the SSID and wireless security details of the access point to which you want to connect.

5. Router Mode

5.1 Overview

The MWR222 is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the MWR222 connects the local network (**LAN1**) to the Internet.

Figure 13 MWR222 Network



Note: The Status screen is shown in the Web Configurator. It varies depending on the device mode of your MWR222.

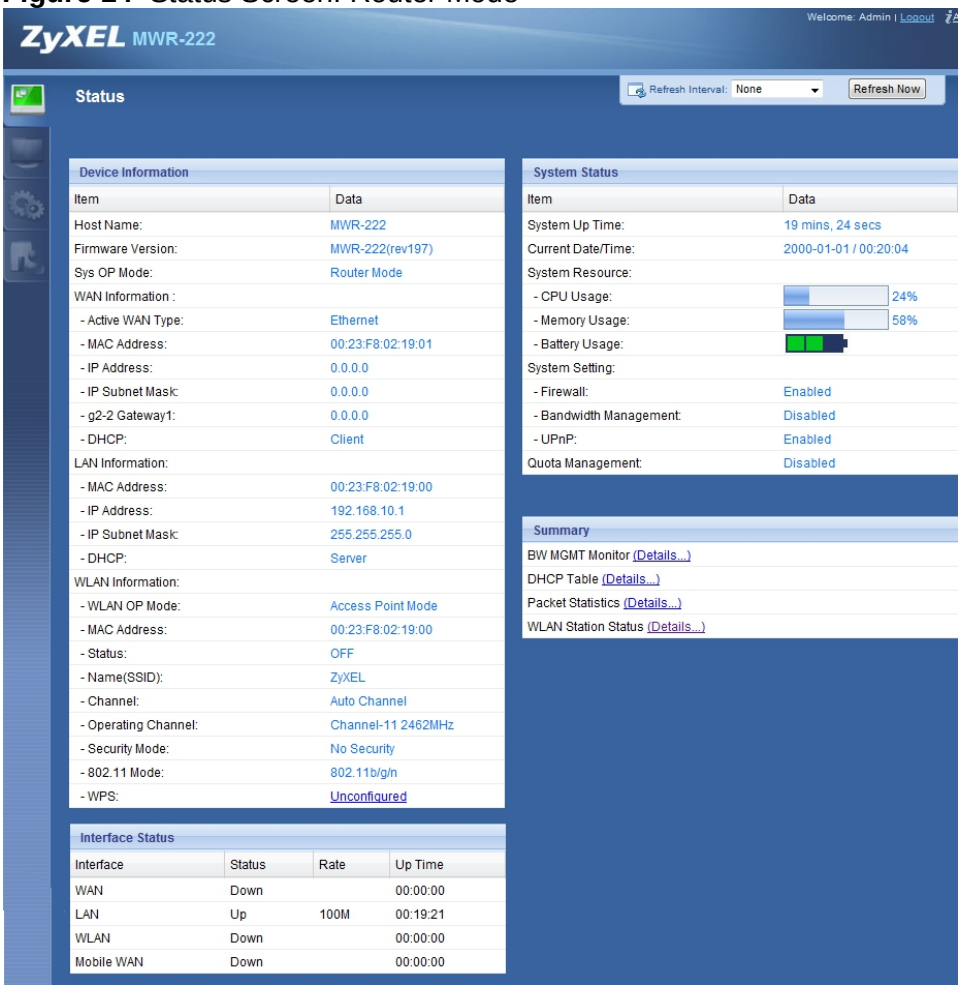
5.2 What You Can Do

Use the **Status** screen to view read-only information about your MWR222.

5.3 Status Screen

Click to open the status screen.

Figure 14 Status Screen: Router Mode



The following table describes the icons shown in the **Status** screen:

Table 9 Status Screen Icon Key: Router Mode

ICON	DESCRIPTION
	Click this icon to view copyright and a link for related product information.
	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the **Monitor** navigation menu.
	Click this icon to see the **Configuration** navigation menu.
	Click this icon to see the **Maintenance** navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 10 Status Screen: Router Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version.

Sys OP Mode	This is the device mode (Device Modes) to which the MWR222 is set – **Router Mode**.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- Active WAN type	This shows the kind of WAN connection is active. There are two types of WAN: Ethernet and Mobile WAN
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Default Gateway	This shows the WAN port's gateway IP address.
- DHCP	This shows the LAN port's DHCP role - **Client** or **Server**.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Server** or **None**.
WLAN Information	
- WLAN OP Mode	This is the device mode (Device Modes) to which the MWR222's wireless LAN is set - **Access Point Mode**.
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **ON** or **OFF**.
- Name (SSID)	This shows a descriptive name used to identify the MWR222 in the wireless LAN.
- Channel	This shows the channel number which you select manually.

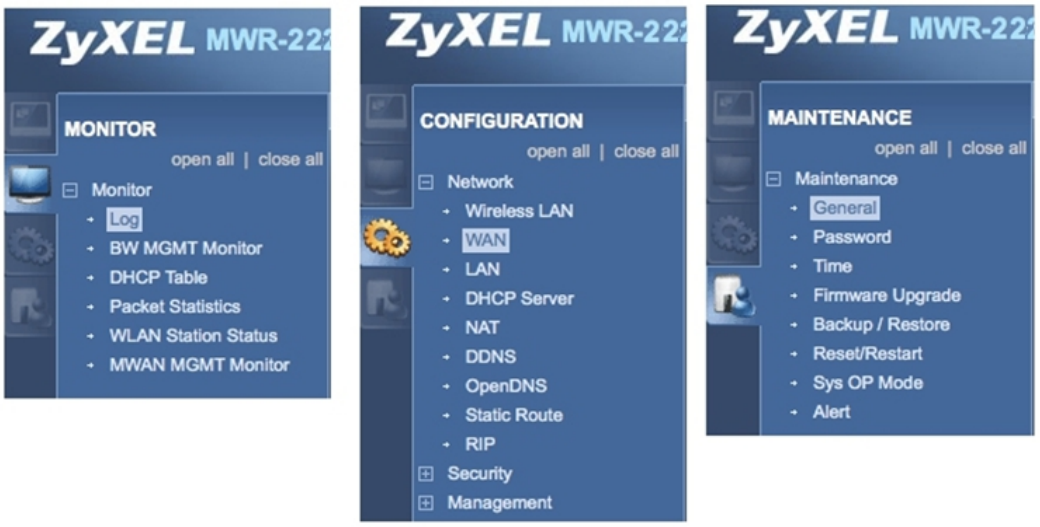
- Operating Channel	This field shows the channel number which the MWR222 is currently using over the wireless LAN.
- Security Mode	This field shows the level of wireless security the MWR222 is using.
- 802.11 Mode	This field shows the wireless standard.
- WPS	This displays **Configured** when the WPS has been set up, or **Unconfigured** if it has not. Click the status to display **Network > Wireless LAN > WPS** screen.
System Status	
Item	This column shows the type of data the MWR222 is recording.
Data	This column shows the actual data recorded by the MWR222.
System Up Time	This is the total time the MWR222 has been on.
Current Date/Time	This field displays your MWR222's present date and time.
System Resource	
- CPU Usage	This field displays the percentage of the MWR222's processing ability that is currently in use. When this percentage is close to 100%, the MWR222 is running at full load, and the throughput is not going to improve any more. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the MWR222 is using.
- Battery Usage	This shows the number of level bars that the battery has.
System Setting	
- Firewall	This shows whether the firewall is enabled or not.
- Bandwidth Management	This shows whether the bandwidth management is enabled or not.
- UPnP	This shows whether UPnP is enabled or not.
- Quota management	This shows the on/off status of data usage management

- Quota Usage	When Quota management is enabled and MWAN is the primary WAN, it shows the number of MBs that are currently being used.
- Percentage Usage	When Quota management is enabled and MWAN is the primary WAN, it shows the percentage of the maximum quota that has been reached.
Interface Status	
Interface	This displays the MWR222 port types. The port types are: **WAN**, **LAN**, **WLAN** and **Mobile WAN.**
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled. For the Mobile WAN, it displays Down when the mobile WAN is not connected, Up when the mobile WAN is connected, and Ready when the mobile WAN is connected in the standby mode.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
BW MGMT Monitor	Click **Details...** to go to the **Monitor > BW MGMT Monitor** screen. Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table	Click **Details...** to go to the **Monitor > DHCP Table** screen. Use this screen to view current DHCP client information.
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen. Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen. Use this screen to view the wireless stations that are currently associated to the MWR222.

5.3.1 Navigation Panel

Use the sub-menus on the navigation panel to configure MWR222 features.

Figure 15 Navigation Panel: Router Mode



The following table describes the sub-menus.

Table 11 Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		This screen shows the MWR222's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
MONITOR		
Log		Use this screen to view the list of activities recorded by your MWR222.
BW MGMT		Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table		Use this screen to view current DHCP client information.
Packet Statistics		Use this screen to view port status and packet specific statistics.

WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the MWR222.
MWAN MGMT Monitor		Use this screen to view the MWAN connection information.
CONFIGURATION		
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the MWR222 to block access to devices or block the devices from accessing the MWR222.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS (Wi-Fi Protected Setup).
	WPS Station	Use this screen to add a wireless station using WPS (Wi-Fi Protected Setup).
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to set up Wireless Distribution System (WDS) on your MWR222. See Chapter 9.12 for more information on the Wireless Distribution System.
WAN	Wired WAN	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address for your Wired WAN connection.
	Mobile WAN	This screen allows you to configure mobile ISP parameters, WAN IP address assignment, Data Usage, Failover, DNS servers, and the WAN MAC address for your Mobile WAN connection.

	Advanced	Use this screen to configure other advanced properties.
	IGMP Snooping	Use this screen to enable IGMP snooping if you have LAN users that subscribe to multicast services.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to have the MWR222 apply IP alias to create LAN subnets.
DHCP Server	General	Use this screen to enable the MWR222's DHCP server. See Chapter 12 for more information about DHCP.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
NAT	General	Use this screen to enable NAT. See Chapter 13 for more information about NAT
	Application	Use this screen to configure servers behind the MWR222.
	Advanced	Use this screen to change your MWR222's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS. See Chapter 14 for more information about DDNS.
OpenDNS	General	Use this screen to set up OpenDNS.
Static Route	IP Static Route	Use this screen to configure IP static routes.
RIP		Use this screen to enable RIPv1 or RIPv2, which are LAN broadcast protocols.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.

	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter		Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		
Bandwidth Management	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
	Monitor	Use this screen to view the amount of network bandwidth that applications running in the network are using.
Remote Management	WWW	Use this screen to be able to access the MWR222 from the LAN, WAN or both.
	SNMP	Use this screen to set up the MWR2215 to manage it using and SNMP v1 management program.
UPnP	General	Use this screen to enable UPnP on the MWR222.

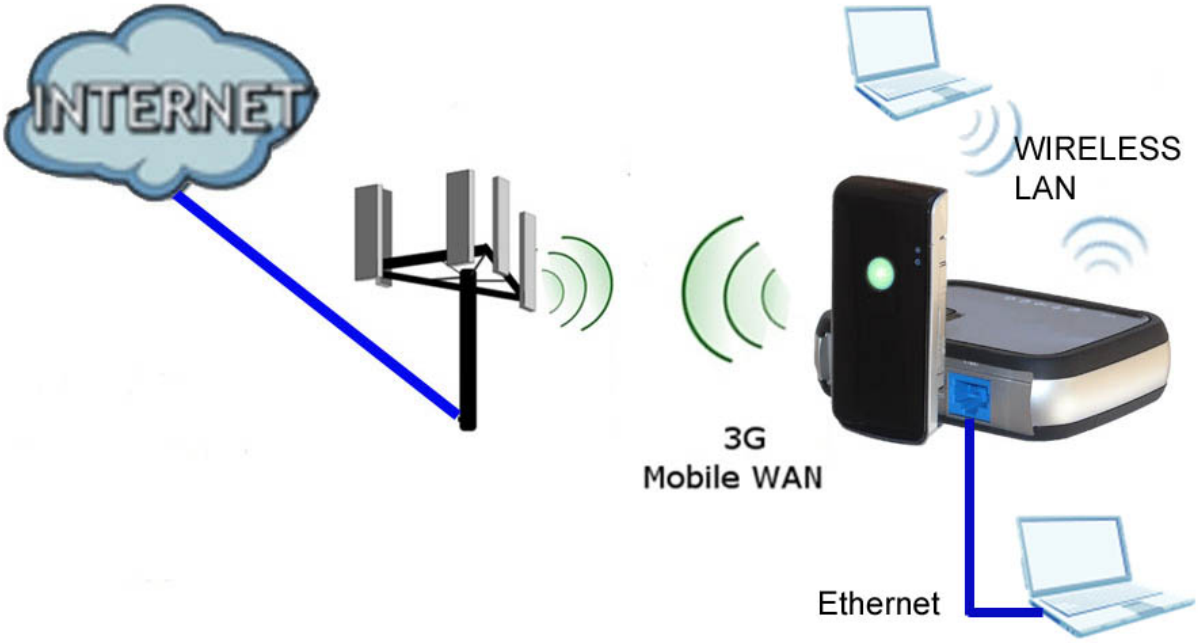
MAINTENANCE		
General		Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your MWR222.
Time	Time Setting	Use this screen to change your MWR222's time and date.
Firmware Upgrade		Use this screen to upload firmware to your MWR222.
Backup/ Restore/ Reset		Use this screen to backup and restore the configuration or reset the factory defaults to your MWR222.
Restart	Restart	This screen allows you to reboot the MWR222 without turning the power off.
Sys OP Mode		This screen allows you to select whether your device acts as a Router or a Access Point.
Alert		Use this screen to set up alerts.

6. Access Point Mode

6.1 Overview

Use your MWR222 as an access point (AP) if you already have a router or gateway on your network. In this mode your MWR222 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 16 Wireless Internet Access in Access Point Mode



Many screens that are available in Router mode are not available in Access Point mode, such as bandwidth management and firewall.

Note: See Chapter 10 for an example of setting up a wireless network in Access Point mode.

6.2 What You Can Do

- Use the **Status** screen to view read-only information about your MWR222.

- Use the **LAN** screen to set the IP address for your MWR222 acting as an access point.

6.3 What You Need to Know

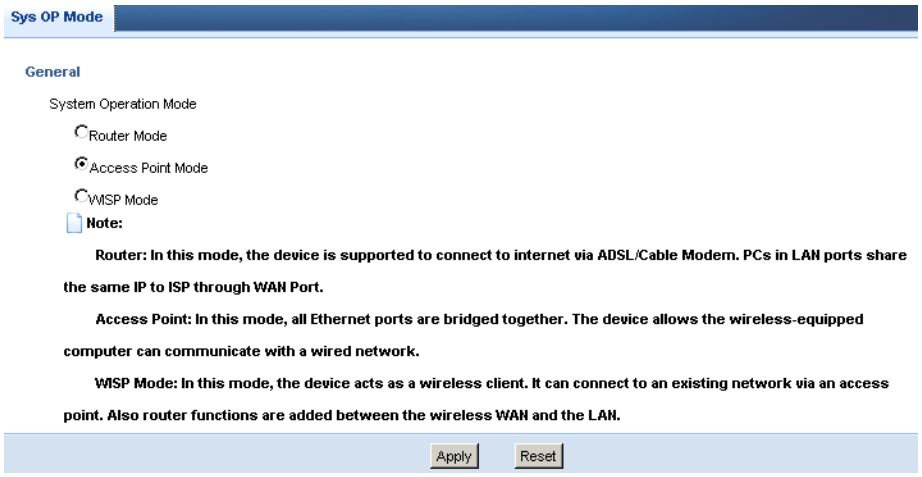
See Chapter 10 for a tutorial on setting up a network with the MWR222 as an access point.

6.3.1 Setting your MWR222 to AP Mode

1. Log into the Web Configurator if you haven't already. See the Quick Start Guide for instructions on how to do this.

2. To use your MWR222 as an access point, go to **Maintenance > Sys OP Mode > General** and select **Access Point mode.**

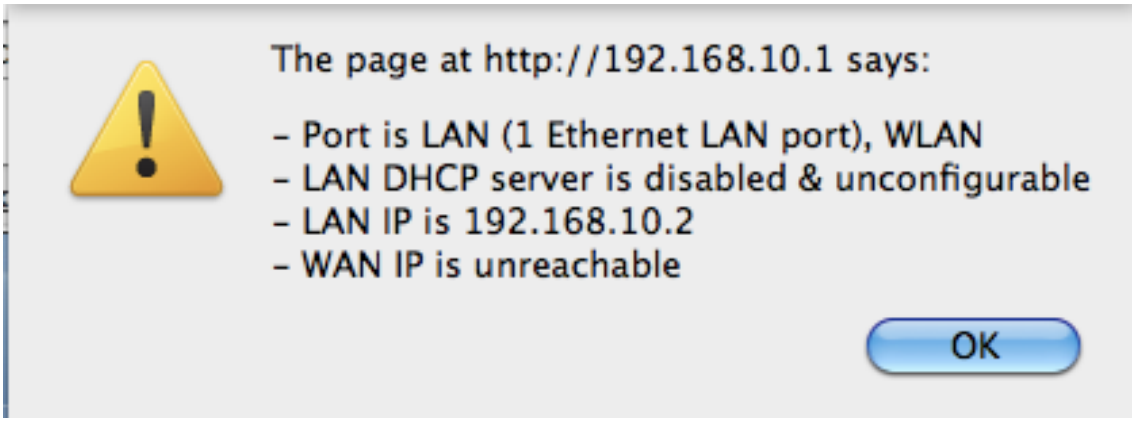
Figure 17 Changing to Access Point mode


Sys OP Mode
General
System Operation Mode
Router Mode
Access Point Mode
WISP Mode
Note:
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.
Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.
WISP Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.
Apply
Reset

Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your MWR222 is already in Access Point mode.

3. When you select **Access Point Mode**, the following pop-up message window appears.

Figure 18 Pop up for Access Point mode


The page at http://192.168.10.1 says:
- Port is LAN (1 Ethernet LAN port), WLAN
- LAN DHCP server is disabled & unconfigurable
- LAN IP is 192.168.10.2
- WAN IP is unreachable
OK

Click **OK**. The Web Configurator refreshes once the change to Access Point mode is successful.

6.3.2 Accessing the Web Configurator in Access Point Mode

Log in to the Web Configurator in Access Point mode, do the following:

1. Connect your computer to the LAN port of the MWR222.
2. The default IP address of the MWR222 is “192.168.10.2”. In this case, your computer must have an IP address in the range between “192.168.10.3” and “192.168.10.254”.
3. Click **Start > Run** on your computer in Windows. Type “cmd” in the dialog box to open the Command Prompt. Once in the Command Prompt, type “ipconfig” and press enter to show your computer’s IP address. If your computer’s IP address is not in the correct range then see Appendix C for information on changing your computer’s IP address.
4. After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “192.168.10.2” as the web address in your web browser.

Note: After clicking Login, see the screens described in the following sections.

6.3.3 Configuring your WLAN, Bandwidth Management and Maintenance Settings

The configuration of wireless, bandwidth management and maintenance settings in **Access Point** mode is the same as for **Router Mode**.

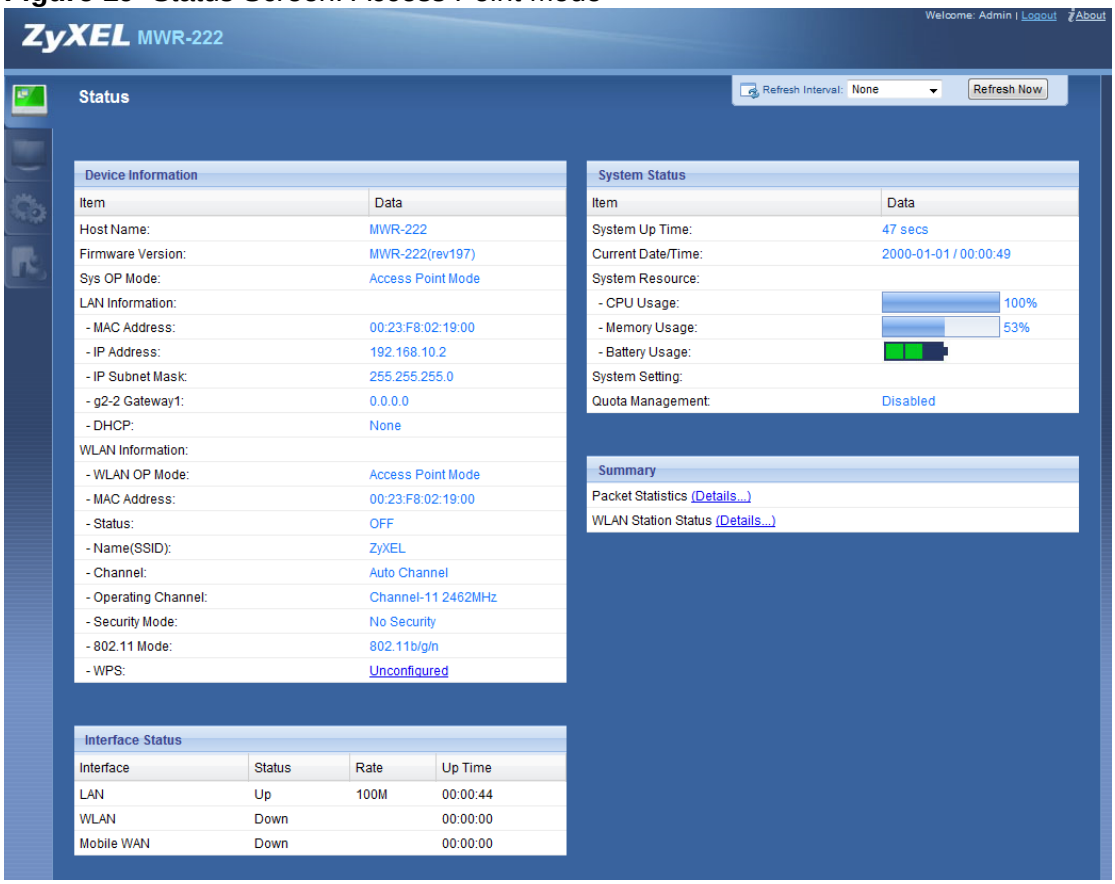
- See Chapter 10 for information on configuring your wireless network.

- See Chapter 20 for information on configuring your Bandwidth Management screen.
- See Maintenance and Troubleshooting for information on configuring your Maintenance settings.

6.4 AP Mode Status Screen

Click to open the **Status** screen.

Figure 19 Status Screen: Access Point Mode



The following table describes the labels shown in the **Status** screen.

Table 12 Status Screen: Access Point Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	

Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Device Modes) to which the MWR222 is set - **Access Point Mode**.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Server, Client or None.**
WLAN Information	
- WLAN OP Mode	This is the device mode (Device Modes) to which the MWR222's wireless LAN is set - **Access Point Mode**.
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **ON** or **OFF**.
- Name (SSID)	This shows a descriptive name used to identify the MWR222 in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the MWR222 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the MWR222 is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display **Network > Wireless LAN > WPS** screen.

System Status	
Item	This column shows the type of data the MWR222 is recording.
Data	This column shows the actual data recorded by the MWR222.
System Up Time	This is the total time the MWR222 has been on.
Current Date/Time	This field displays your MWR222's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the MWR222's processing ability is currently used. When this percentage is close to 100%, the MWR222 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
- Memory Usage	This shows what percentage of the heap memory the MWR222 is using.
System Setting	
Interface Status	
Interface	This displays the MWR222 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen. Use this screen to view port status and packet specific statistics.

WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen. Use this screen to view the wireless stations that are currently associated to the MWR222.

6.4.1 Navigation Panel

Use the menu in the navigation panel to configure MWR222 features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

Figure 20 Menu: Access Point Mode

Refer to **Table 11** Navigation Panel: Router Mod for descriptions of the labels shown in the **Navigation** panel.

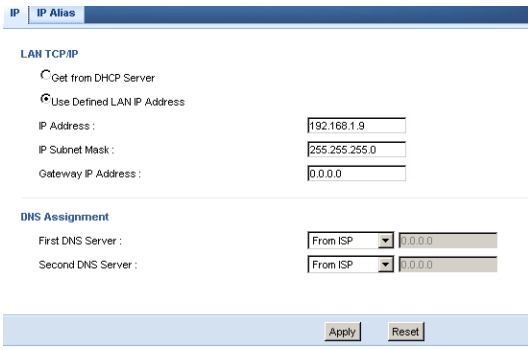
6.5 LAN Screen

Use this section to configure your LAN settings while in **Access Point** mode.

Click **Network > LAN** to see the screen below.

Note: If you change the IP address of the MWR222 in the screen below, you will need to log into the MWR222 again using the new IP address.

Figure 21 Network > LAN > IP



The table below describes the labels in the screen.

Table 13 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	Click this to deploy the MWR222 as an access point in the network. When you enable this, the MWR222 gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the MWR222 can now access the network (i.e., the Internet if the IP address is given by the ISP). The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the MWR222. You need to reset the MWR222 to be able to access the Web Configurator again. Also when you select this, you cannot enter an IP address for your MWR222 in the field below.
Use Defined LAN IP Address	Click this if you want to specify the IP address of your MWR222. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.10.2. If you change the IP address you will have to log in again with the new IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your MWR222 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the MWR222.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP or network administrator gave you one) in this field.
DNS Assignment	

First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

7. WISP Mode

7.1 Overview

Your MWR222 can receive a WAN IP address from an 802.11 WIFI connection. In WISP mode, it can connect to an existing network via an access point. Use this mode if your Internet Service Provider allows you to connect to their network via 802.11 WIFI. This mode is meant to allow a Public IP address to be received via a Wi-Fi connection. If when you connect your MWR222 to an access point you receive a Private IP address (i.e. 192.168.10.1), you may be able to get on line, but certain applications (gaming, video streaming) may not work.

The WISP mode is not a simple “Wireless Bridge” because in a wireless bridge there is no routing done on the device. In WISP mode the MWR222 still acts as a router/firewall and will therefore cause problems if connected to another router/firewall. The MWR222 must be connecting to some type of non-routing wireless access point in order to connect properly.

In the example below, the MWR222 is configured in WISP mode The wireless router has one clients that need to connect to the Internet. The MWR222 wirelessly connects to the available access point

Figure 22 WISP Mode

After the MWR222 and the access point connect, the MWR222 acquires its Public WAN IP address from the access point. The clients of the MWR222 can now surf the Internet.

7.2 What You Can Do

- Use the **Status** screen to view read-only information about your MWR222.
- Use the **LAN** screen to set the IP address for your MWR222 acting as an access point.
- Use the **Wireless LAN** screen to associate your MWR222 (acting as a wireless client) with an existing access point.

7.3 What You Need to Know

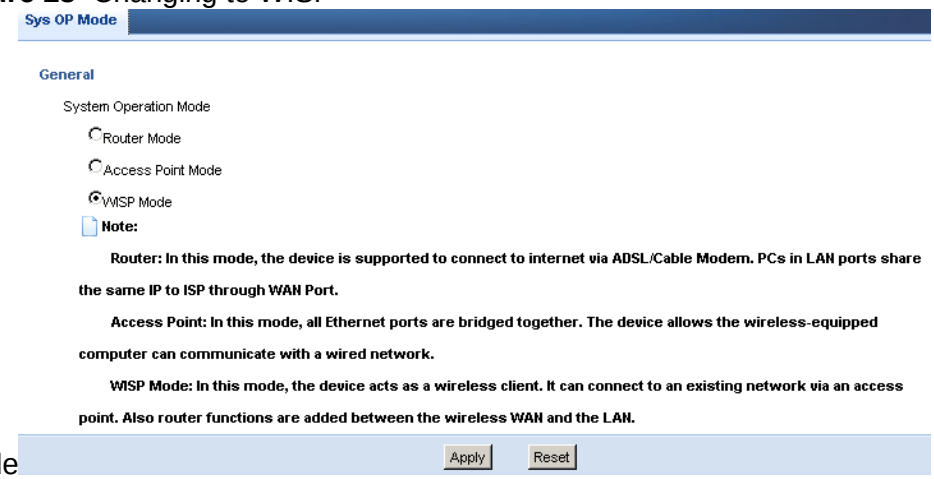
With the exception of the **LAN** screen, the **Monitor**, **Configuration** and **Maintenance** screens in WISP mode are similar to the ones in Router Mode.

7.3.1 Setting your MWR222 to WISP Mode

1. Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.

2. To set your MWR222 to **AP Mode**, go to **Maintenance > Sys OP Mode > General** and select **WISP Mode.**

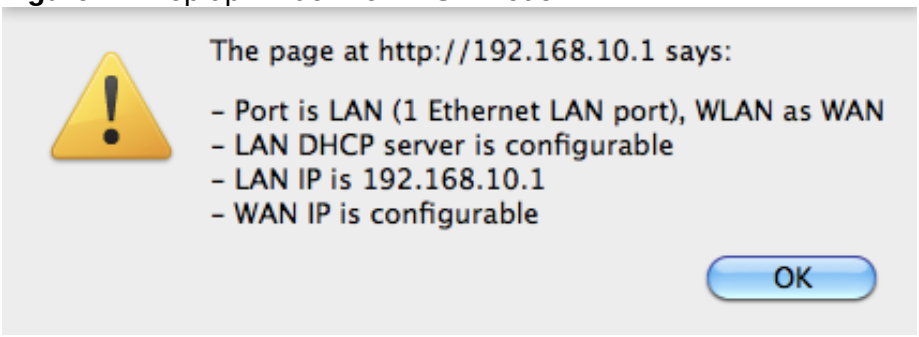
Figure 23 Changing to WISP mode


Sys OP Mode
General
System Operation Mode
Router Mode
Access Point Mode
WISP Mode
Note:
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.
Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.
WISP Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.
Apply
Reset

Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your MWR222 is already in WISP mode.

3. When you select **WISP Mode**, the following pop-up message window appears.

Figure 24 Pop up window for WISP mode


The page at http://192.168.10.1 says:
- Port is LAN (1 Ethernet LAN port), WLAN as WAN
- LAN DHCP server is configurable
- LAN IP is 192.168.10.1
- WAN IP is configurable
OK

Click **OK**. The Web Configurator refreshes once the change to WISP mode is successful.

7.3.2 Accessing the Web Configurator in WISP Mode

To login to Web Configurator in WISP mode, do the following

1. Connect your computer to the LAN port of the MWR222.
2. The default IP address of the MWR222 is “192.168.10.1”. If you did not change this, you can use the same IP address in WISP mode. Open a web browser such as Internet Explorer and type “192.168.10.1” as the web address in your web browser.

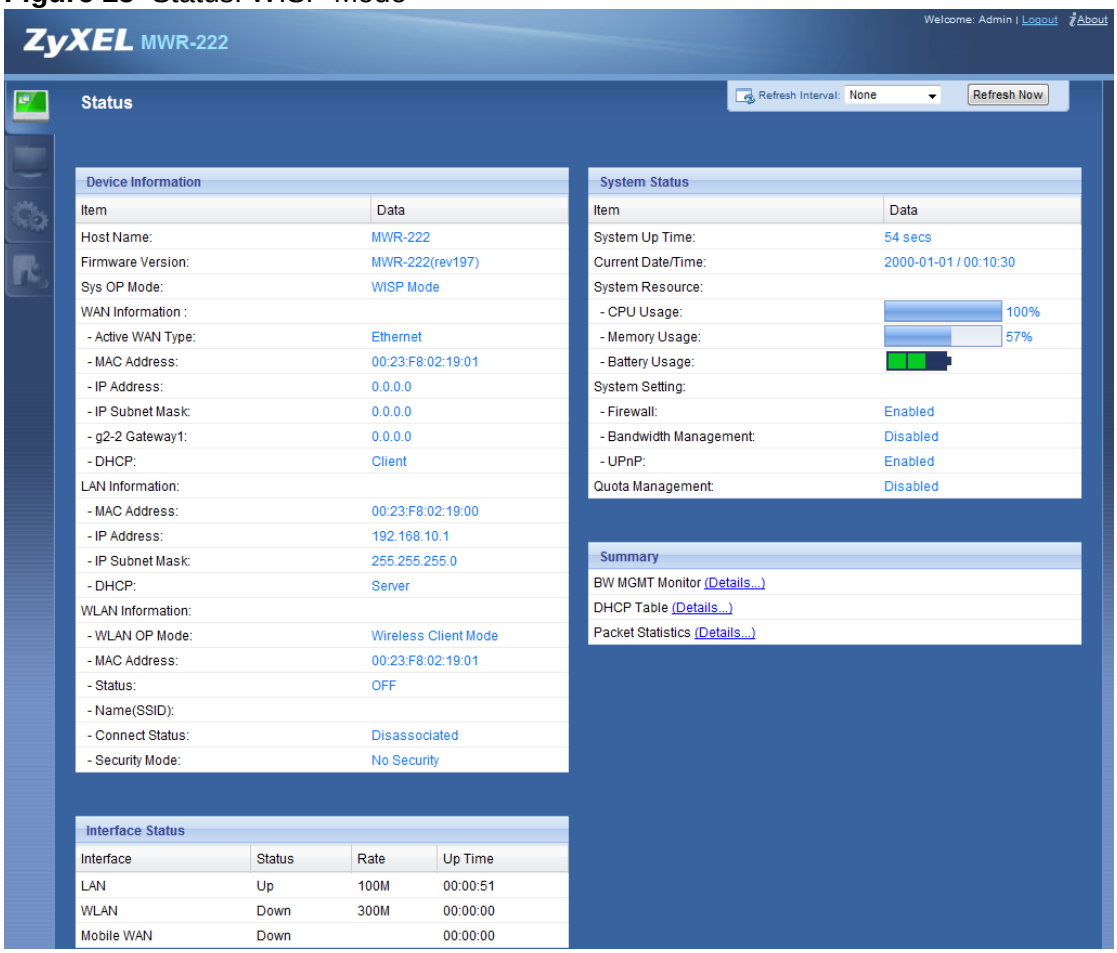
If you changed the IP address of your MWR222 while in Router Mode, use this IP address in WISP mode. The WISP mode IP address is always the same as the Router mode IP address.

Note: After clicking Login, see the screens described in the sections following this. The WISP mode means using Wi-Fi as WAN, NOT 3G as WAN.

7.4 WISP Mode Status Screen

Click to open the status screen.

Figure 25 Status: WISP Mode



The following table describes the labels shown in the **Status** screen.

Table 14 Status Screen: WISP Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.

Sys OP Mode	This is the device mode (Device Modes) to which the MWR222 is set - **WISP Mode**.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Default Gateway	This shows the WAN port's gateway IP address.
- DHCP	This shows the LAN port's DHCP role - **Client** or **Server**.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Server** or **None**.
WLAN Information	
- WLAN OP Mode	This is the device mode (Device Modes) to which the MWR222's wireless LAN is set - **Access Point Mode**.
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **ON** or **OFF**.
- Name (SSID)	This shows a descriptive name used to identify the MWR222 in the wireless LAN.
- Connect Status	This shows whether or not the MWR222 has successfully associated with an access point - **Connected** or **Disassociated**.
- Security Mode	This shows the level of wireless security the MWR222 is using.

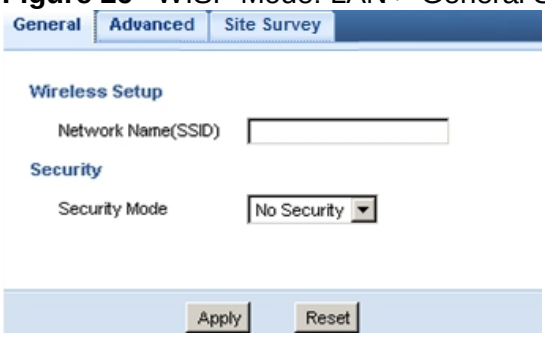
- 802.11 Mode	This shows the wireless standard.
System Status	
Item	This column shows the type of data the MWR222 is recording.
Data	This column shows the actual data recorded by the MWR222.
System Up Time	This is the total time the MWR222 has been on.
Current Date/Time	This field displays your MWR222's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the MWR222's processing ability is currently used. When this percentage is close to 100%, the MWR222 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
- Memory Usage	This shows what percentage of the heap memory the MWR222 is using.
System Setting	
- Firewall	This shows whether the firewall is enabled or not.
- Bandwidth Management	This shows whether the bandwidth management is enabled or not.
- UPnP	This shows whether UPnP is enabled or not.
- Configuration Mode	This shows the web configurator mode you are viewing - **Expert**.
Interface Status	
Interface	This displays the MWR222 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.

Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
BW MGMT Monitor	Click **Details...** to go to the **Monitor > BW MGMT Monitor** screen. Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table	Click **Details...** to go to the **Monitor > DHCP Table** screen. Use this screen to view current DHCP client information.
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen. Use this screen to view port status and packet specific statistics.

7.5 Wireless LAN General Screen

Use this screen to configure the wireless LAN settings of your MWR222. Go to **Configuration > Wireless LAN > General** to open the following screen.

Figure 26 WISP Mode: LAN > General Screen



The following table describes the labels in this screen.

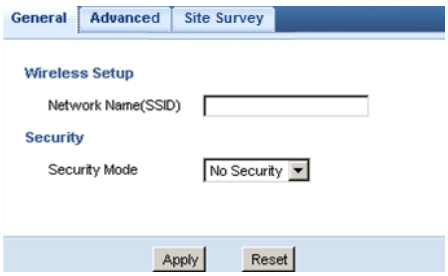
Table 15 WISP Mode: LAN > General Screen

LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select the security mode of the access point to which you want to connect.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.1 No Security

Use this screen if the access point to which you want to connect does not use encryption.

Figure 27 No Security (WISP)



The following table describes the labels in this screen.

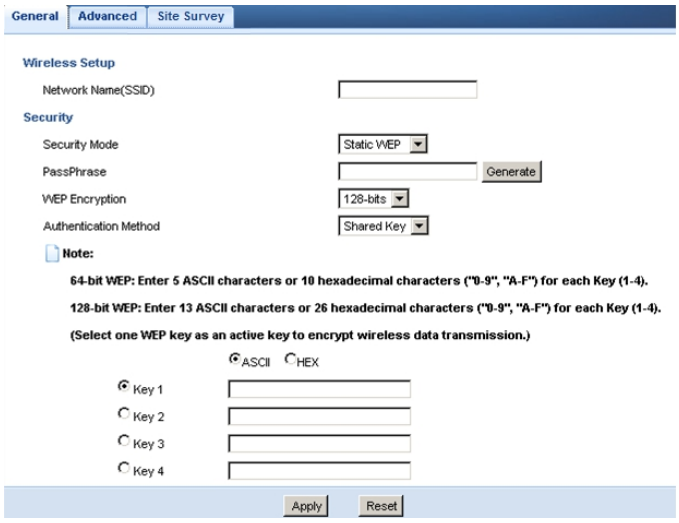
Table 16 No Security (WISP)

LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select **No Security** in this field.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.2 Static WEP

Use this screen if the access point to which you want to connect to uses WEP security mode.

Figure 28 WEP (WISP)



The following table describes the labels in this screen.

Table 17 WEP (WISP)

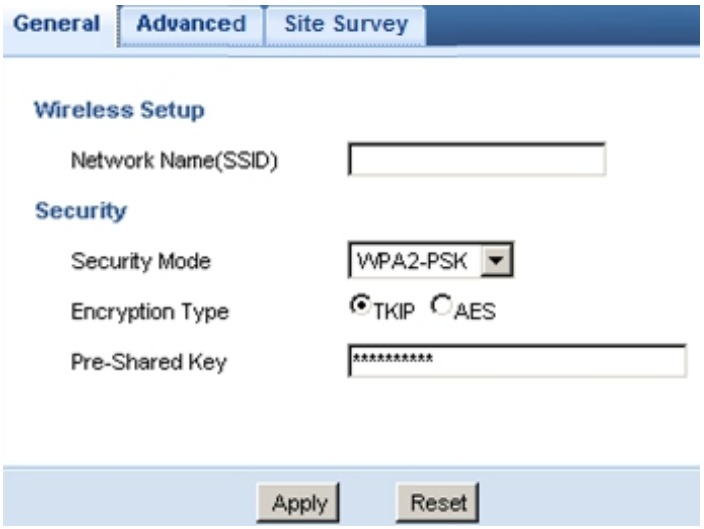
LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select **Static WEP** to enable data encryption.
Passphrase	Enter a Passphrase (up to 26 printable characters) and click **Generate**. A passphrase functions like a password. In WEP security mode, it is further converted by the MWR222 into a complicated string that is referred to as the “key.” This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Auto** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** unless you want to force a key verification before communication between the wireless client and the ZyXEL device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

Key 1 to Key 4	The WEP keys are used to encrypt data. Both the MWR222 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.3 WPA(2)-Personal/Enterprise

Use this screen if the access point to which you want to connect uses WPA(2)-Personal/Enterprise security mode.

Figure 29 WPA-PSK/WPA2Personal/Enterprise (WISP)



The following table describes the labels in this screen. .

Table 18 WPA-PSK/WPA2-PSK (WISP)

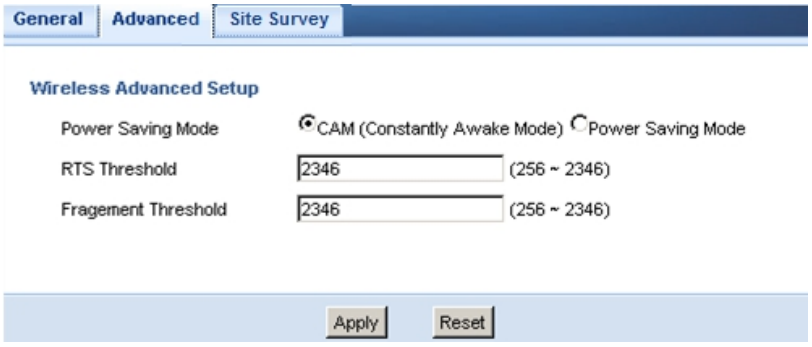
LABEL	DESCRIPTION
Wireless Setup	

Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	**WPA-PSK / WPA2-PSK** uses a simple common password for authentication. Type the pre-shared key employed by the access point to which you want to connect.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.4 Advance Screen

Use this screen to enable the power saving mode of your MWR222. Go to **Configuration > Wireless LAN** to open the following screen.

Figure 30 Configuration > Wireless LAN > Advance Screen (WISP)



The following table describes the labels in this screen.

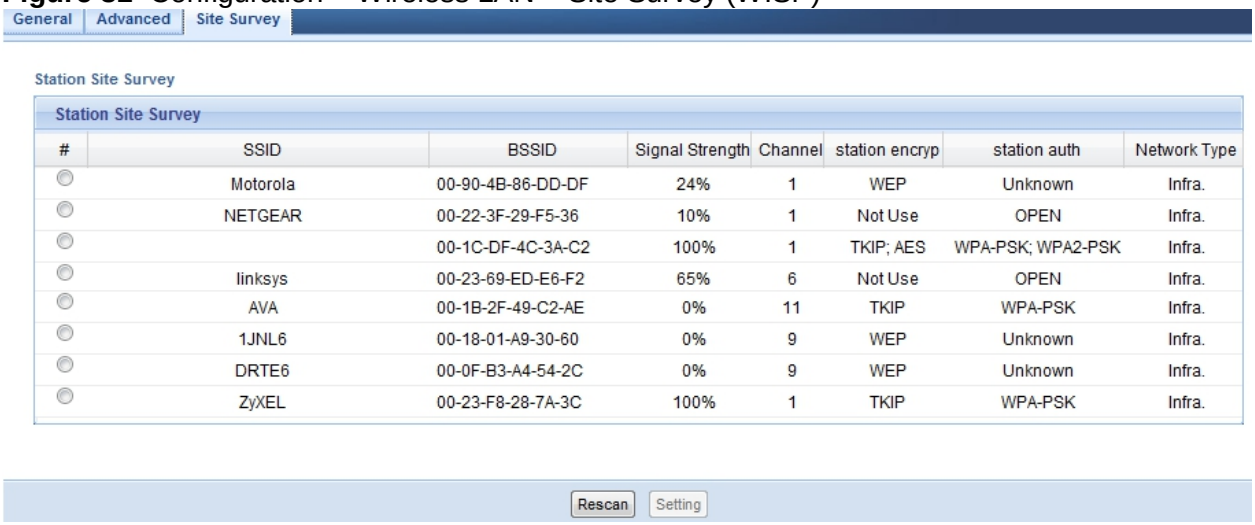
Table 19 Configuration > Wireless LAN > Advance Screen (WISP)

LABEL	DESCRIPTION
Power Saving Mode	Select **CAM (Constantly Awake Mode)** if you do not want your MWR222 to go to “sleep” when no wireless activity is detected in the Wireless LAN. Select **Power Saving Mode** if you want the MWR222 to go to sleep when no wireless connection is needed for a period of time. This means the MWR222 consumes less electrical power.
RTS Threshold	This is the maximum data fragment size that can be sent in a wireless network before the AP fragments the packet into smaller data frames.
Fragment Threshold	This value controls how often wireless clients must get permission to send information to the AP. The lower the value, the more often the wireless clients must get permission. If this value is greater than the fragmentation threshold value, then wireless clients never have to get permission to send information to the AP.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.5 Site Survey

Use this screen to view nearby wireless networks and select one to connect to in WISP mode. Go to **Configuration > Wireless LAN** to open the following screen.

Figure 31 Configuration > Wireless LAN > Site Survey (WISP)


General
Advanced
Site Survey
Station Site Survey
Station Site Survey
SSID BSSID Signal Strength Channel station encryp station auth Network Type
Motorola 00-90-4B-86-DD-DF 24% 1 WEP Unknown Infra.
NETGEAR 00-22-3F-29-F5-36 10% 1 Not Use OPEN Infra.
00-1C-DF-4C-3A-C2 100% 1 TKIP; AES WPA-PSK; WPA2-PSK Infra.
linksys 00-23-69-ED-E6-F2 65% 6 Not Use OPEN Infra.
AVA 00-1B-2F-49-C2-AE 0% 11 TKIP WPA-PSK Infra.
1JNL6 00-18-01-A9-30-60 0% 9 WEP Unknown Infra.
DRTE6 00-0F-B3-A4-54-2C 0% 9 WEP Unknown Infra.
ZyXEL 00-23-F8-28-7A-3C 100% 1 TKIP WPA-PSK Infra.
Rescan
Setting

The following table describes the labels in this screen.

Table 20 Configuration > Wireless LAN > Site Survey (WISP)

LABEL	DESCRIPTION
Station Site Survey	
#	Use this option to select the wireless network you want to connect to.
SSID	This displays the Network Name (SSID) of the wireless networks close to you.
BSSID	This displays the MAC address of the wireless device listed.
Signal Strength	This displays the strength of the wireless network.
Channel	This displays the wireless channel used by the wireless network.
Station Encryp	This displays the encryption type used by the wireless network.
Station Auth	This displays the authentication method used by the wireless network.
Network Type	This displays the network type being used by the wireless network.
Rescan	Scan for wireless networks.

Setting	Click this after selecting a network to set the

8 Tutorials

8.1 Overview

This chapter provides tutorials for your MWR222 as follows:

- Wired and Wireless 3G connection to the Internet
- Connecting to the Internet from an Access Point
- Configuring Wireless Security Using WPS
- 8.5 Enabling and Configuring Wireless Security (N

8.2 Connecting to the Internet

When first connecting your MWR222 to a wired or wireless 3G Internet connection, you will want to ensure you are connecting with the best possible settings for the modem being used. This section will give you a general example of the best practices for the most common Internet connection methods.

MWR222 uses one active WAN connection at any given time. If both wired WAN and mobile WAN are connected to the Internet, MWR222 will use the wired WAN for Internet communication. If the wired WAN connection is dropped for any reason, MWR222 will automatically use mobile WAN for Internet communication.

On the other hand, if the mobile WAN is the only Internet connection, then the wired WAN is connected, MWR222 will automatically use the wired WAN for Internet communication.

8.2.1 DSL Modem

If your internet connection comes from a DSL modem you will want to follow these steps to best prepare your modem to connect with the MWR222.

- Contact your ISP (Internet Service Provider) and ask them to help you “bridge” your DSL modem.
- Find out from your ISP what the “PPPoE Username and Password” are for your Internet connection.
- Once the DSL modem has been bridged, connect it (by Ethernet cord) to the WAN port of the MWR222 (MWR222 has only one Ethernet port, and it is configured to be a LAN port by default. So user has to change the configuration first so that the Ethernet port can act as the WAN port. Once

this is done user can no longer use the wired connection for the web configurator.)

- Open your browser and log into the MWR222. Click on Configuration > Network > Wired WAN, for the encryption select “PPPoE” and enter your PPPoE “Username and Password.”

8.2.2 Cable Modem

- Connect the cable modem to your MWR222 on the WAN port. (MWR222 has only one Ethernet port, and it is configured to be a LAN port by default. So user has to change the configuration first so that the Ethernet port can act as the WAN port. Once this is done user can no longer use the wired connection for the web configurator.)

- Unplug the power to your cable modem. Depending on your cable modem, it may also have a backup battery inside. Remove this battery and completely power down the cable modem. Let it sit from 2 to 3 minutes and then reconnect the battery and power to the cable modem.

- If the router is set with its default settings it should automatically connect to the Internet.

8.2.3 3G USB Adapter

- Activate the 3G USB adapter on a PC first, using the software provided by the ISP.

- Connect the 3G USB adapter to the USB port on the back of the MWR222

- Log into your MWR222 using your computer’s browser.

- Click on the Configuration tab at the left side of the screen.

- Click on “Network” under the configuration tab, and then click on “WAN”.

- On the WAN configuration page, click on the Mobile WAN tab at the top of the page. Then fill in the account information you obtained from the mobile broad band ISP. Make sure you check “Nailed-Up Connection.”

- After filling in all the account information, click the “Connect” button to save the information to the router’s memory and make the wireless 3G connection.

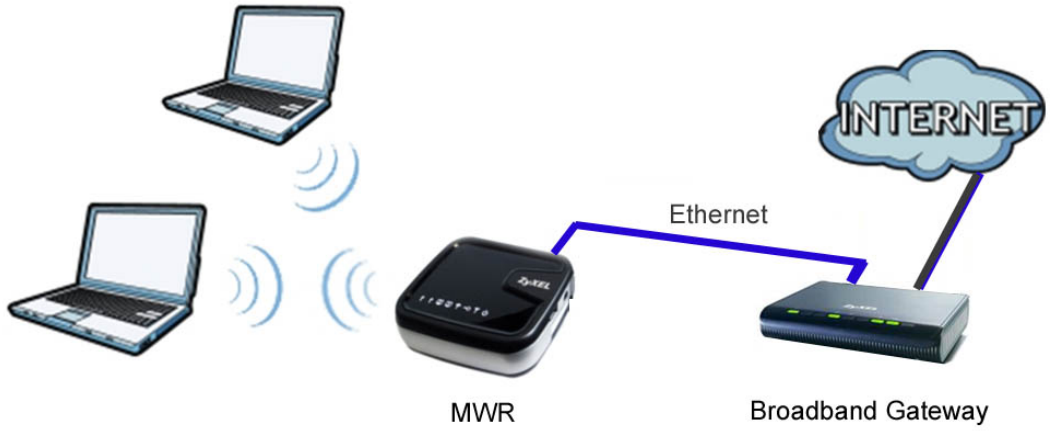
- The USB LED starts to blink fast, indicating MWR222 is connecting. When the mobile WAN is connected, the USB LED changes solid on. However, if the Ethernet port is configured to WAN, and is connected to a wired WAN, the mobile WAN will be used as the backup WAN so the USB LED shows slow blinking.

- When a 3G USB adapter is removed from the USB port, the USB LED will turn off in about 10 seconds. Do not re-insert the 3G USB adapter into the USB port until the USB LED has turned off, or 10 seconds have passed.
- The Data Usage Count, if enabled, will be written to MWR222 internal storage when the 3G USB adapter is removed. Do not power off MWR222 before the USB LED has turned off, or 10 seconds have passed.

8.3 Connecting to Internet from an Access Point

This section gives you an example of how to set up an access point (**AP**) and wireless client (a notebook (**B**), in this example) for wireless communication. **B** can access the Internet through the access point wirelessly When the MWR is configured in AP mode, it has to connect to a broadband gateway (wired or wireless router with broadband connection) . Local computer(s) can get IP via wireless connection passed by MWR from the broadband gateway, then gain Internet access.

Figure 32 Wireless Access Point mode



Internet

8.4 Configuring Wireless Security Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the MWR222 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See 8.4.1 Push Button Configuration (PBC).This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the MWR222's interface. See 8.4.2 PIN Configuration. This is the more secure method, since one device can authenticate the other.

8.4.1 Push Button Configuration (PBC)

1. Make sure that your MWR222 is turned on and that it is within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into MWR222's Web Configurator and press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

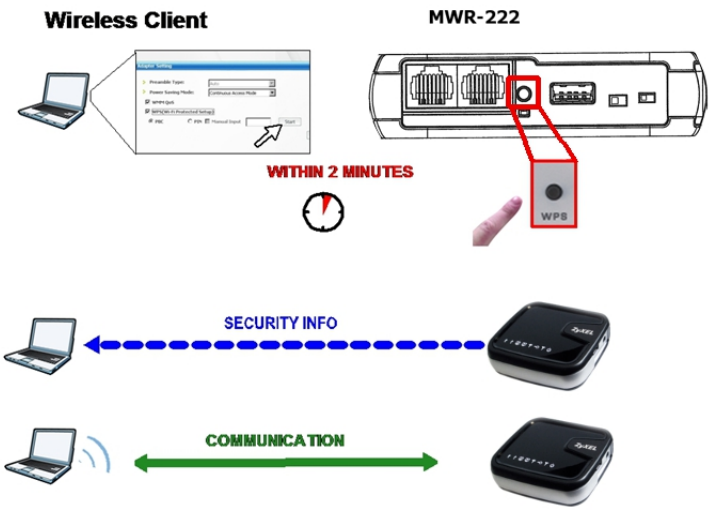
Note: Your MWR222 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The MWR222 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the MWR222 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both MWR222 and wireless client (the NWD210N in this example).

Figure 33 Example WPS Process: PBC Method



8.4.2 PIN Configuration

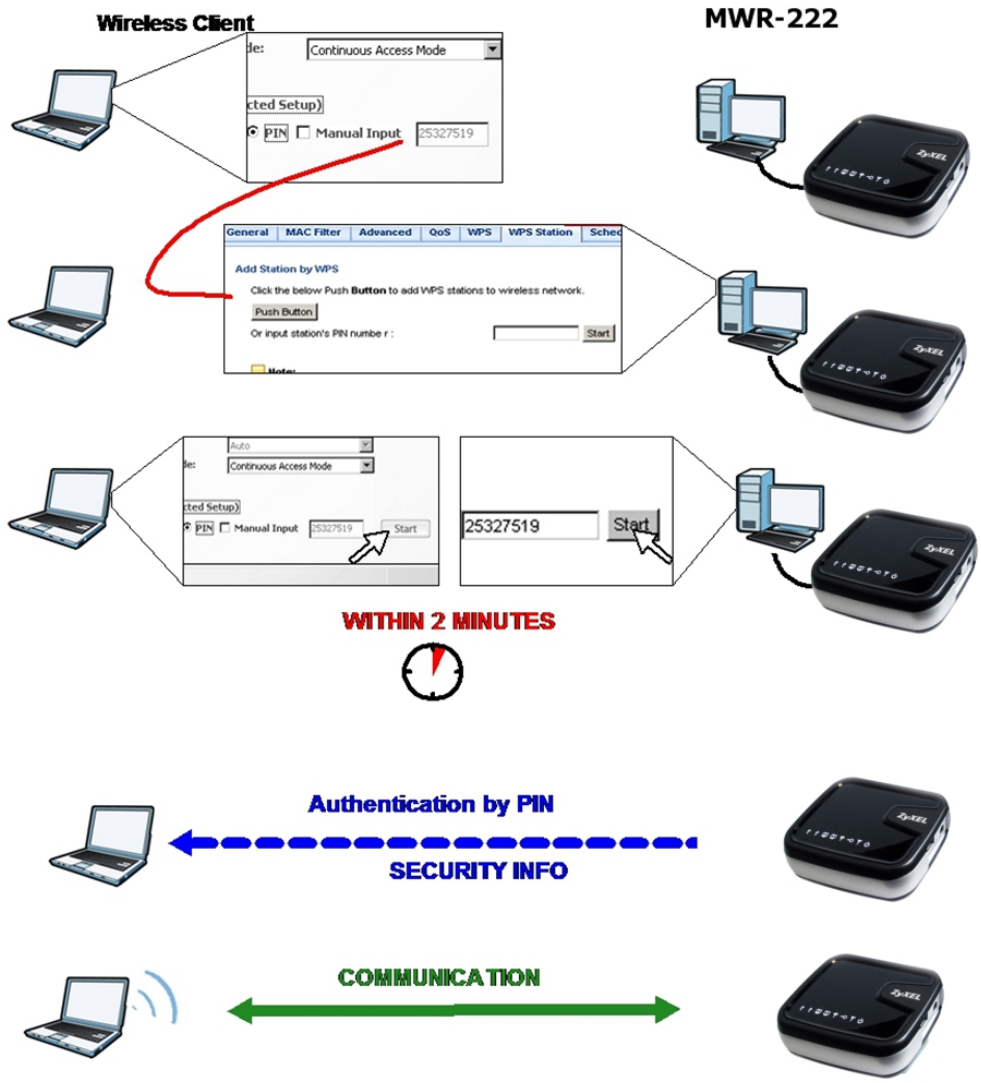
When you use the PIN configuration method, you need to use both MWR222's configuration interface and the client's utilities.

1. Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the MWR222.
3. Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the MWR222's **WPS Station** screen within two minutes.

The MWR222 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the MWR222 securely.

The following figure shows you how to set up wireless network and security on MWR222 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 34 Example WPS Process: PIN Method



8.5 Enabling and Configuring Wireless Security (No WPS)

This example shows you how to configure wireless security settings with the following parameters on your MWR222.

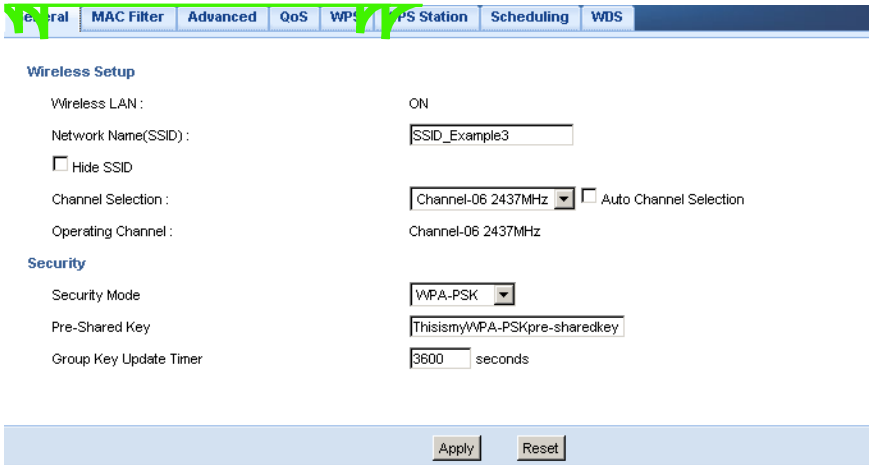
SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your MWR222.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection.

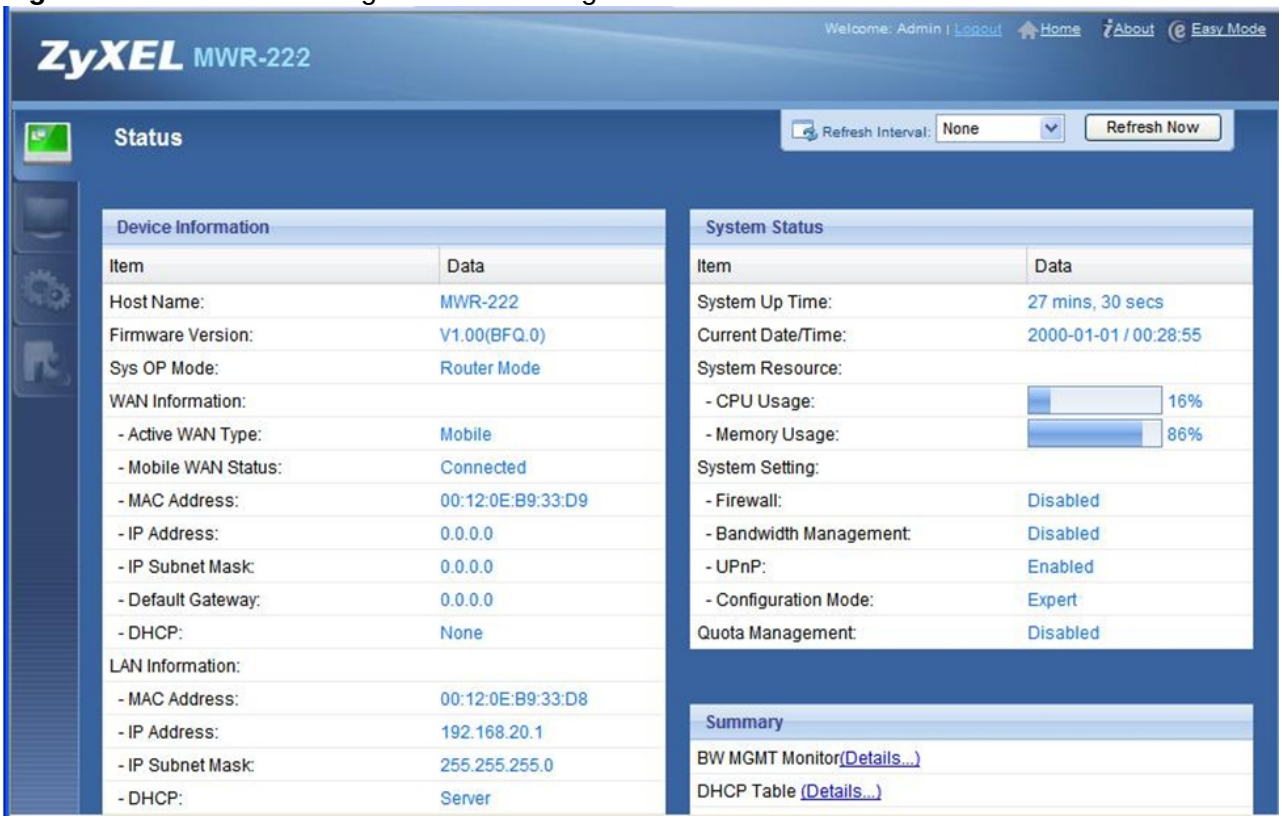
1. Open the **Wireless LAN > General** screen in the AP's Web Configurator.
2. Make sure the **Enable Wireless LAN** check box is selected.
3. Enter **SSID_Example3** as the SSID and select a channel.
4. Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 35 Tutorial: Network > Wireless LAN > General



5. Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 36 Tutorial: Checking Wireless Settings



8.5.1 Configure Your Notebook

Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

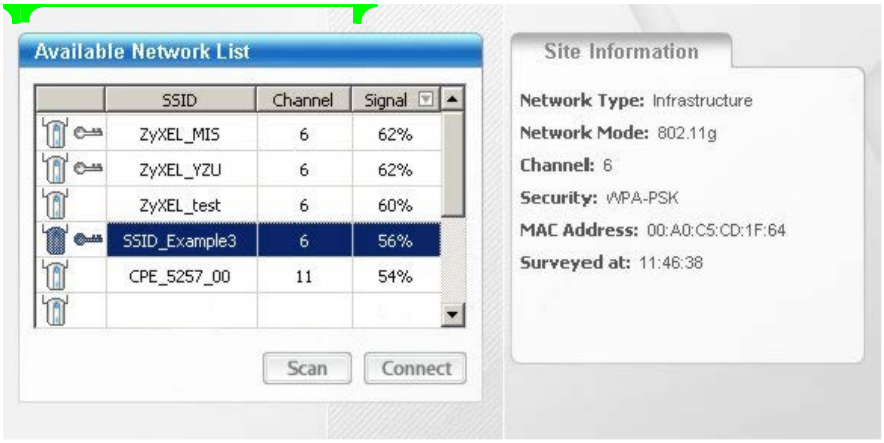
1. The MWR222 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2. Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3. After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

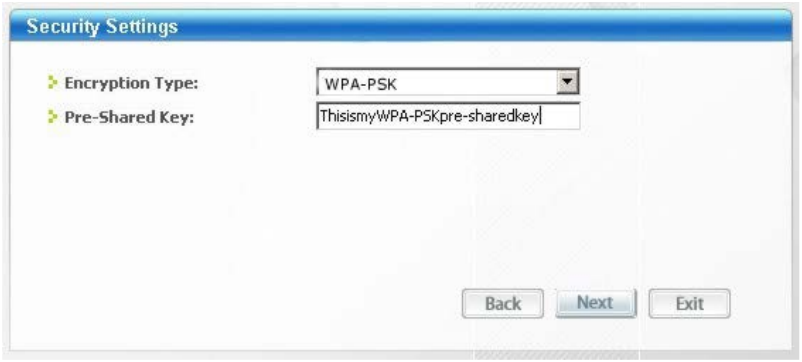
4. Select SSID_Example3 and click **Connect**.

Figure 37 Connecting a Wireless Client to a Wireless Network



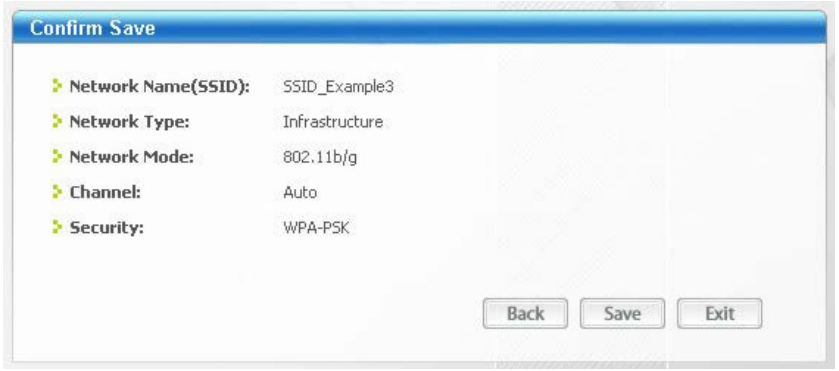
5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 38 Security Settings



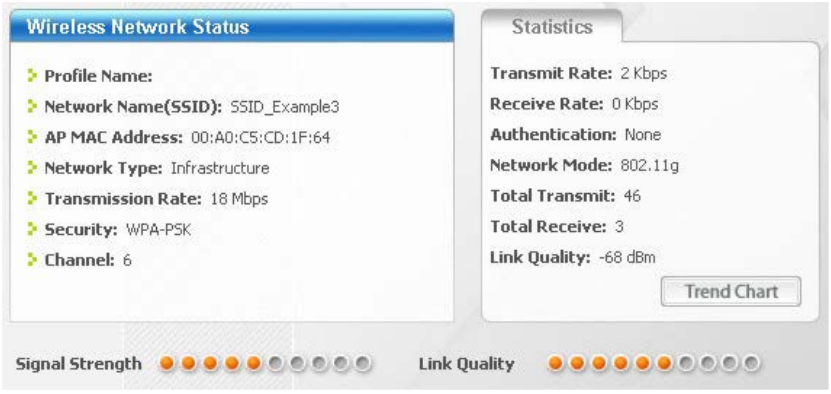
6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 39 Confirm Save



7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 40 Link Status



If your connection is successful, open your Internet browser and enter http://us.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

Part II
Network

Wireless LAN

WAN

LAN

DHCP Server

Network Address Translation (NAT)

Dynamic DNS

OpenDNS

Static Route

RIP

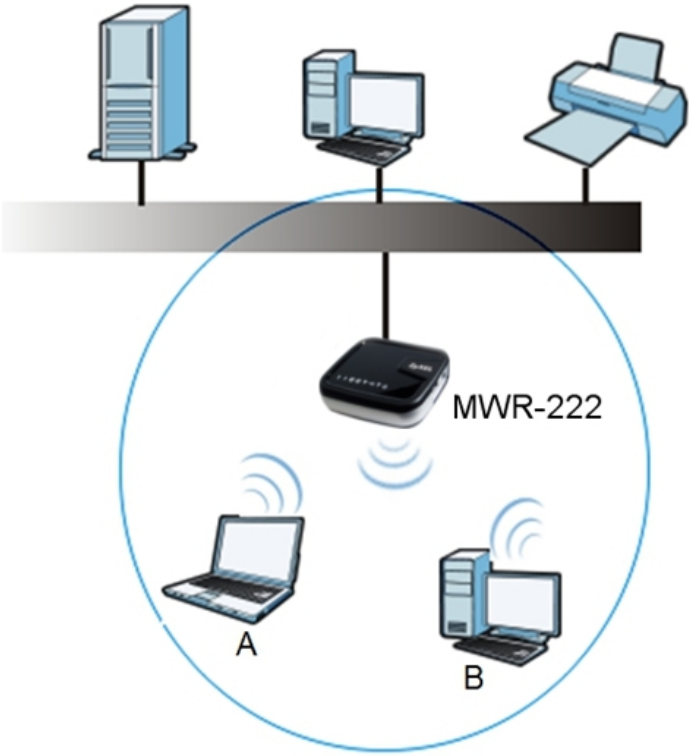
9 Wireless LAN

9.1 Overview

This chapter discusses how to configure the wireless network settings in your MWR222. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 41 Example of a Wireless



Network

The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your MWR222 is the AP.

9.2 What You Can Do

- **Use the** General **screen** to enable the Wireless LAN, enter the SSID and select the wireless security mode.
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the MWR222.
- Use the **Advanced** screen to allow wireless advanced features, such as intra-BSS networking and set the RTS/CTS Threshold.
- Use the **QoS** screen to set priority levels to services, such as e-mail, VoIP, chat, and so on.
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen to add a wireless station using WPS.
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off.
- Use the **WDS** screen to configure Wireless Distribution System on your MWR222.

9.3 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

9.3.1 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

9.3.1.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

9.3.1.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

9.3.1.3 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication.

Table 21 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION
Weakest	No Security
↕	WEP

[1]Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2]Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

	WPA-Personal (TKIP) WPA-Enterprise
Strongest	WPA2-Personal (AES) WPA2-Enterprise

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-Personal/Enterprise** or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

When you select **WPA2-Personal/Enterprise** in your MWR222, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-Personal/Enterprise** (depending on the type of wireless network login) and select the **WPA Compatible** option in the MWR222.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

9.3.1.4 WPS

Wi-Fi Protected Setup (WPS) is an industry standard specification, defined by the Wi-Fi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves.

9.3.1.5 WDS

Wireless Distribution System or WDS security is used between bridged APs. It is independent of the security between the wired networks and their respective APs. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key.

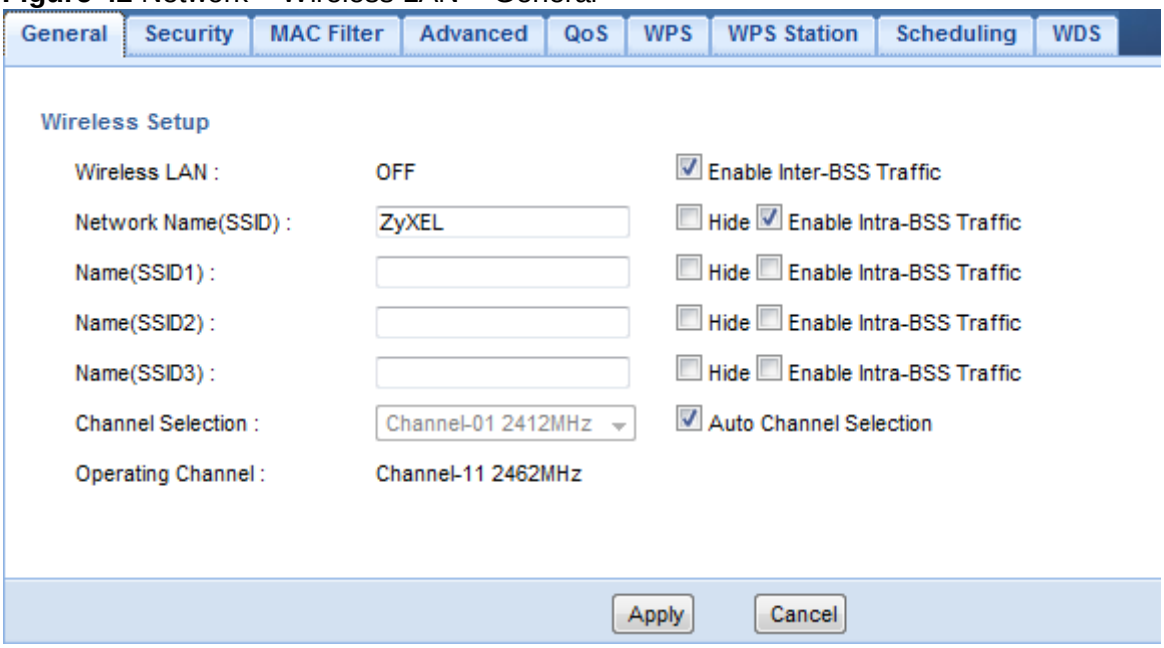
9.4 General Wireless LAN Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the MWR222 from a computer connected to the wireless LAN and you change the MWR222's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the MWR222's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 42 Network > Wireless LAN > General



The following table describes the general wireless LAN labels in this screen.

Table 22 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	This is turned on by default. You can turn the wireless LAN on or off using the switch at the rear panel of the MWR222. The current wireless state is reflected in this field.

Network Name(SSID) Name (SSID1, SSID2, SSID3)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the MWR222 must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. This option is only available if **Auto Channel Selection** is disabled. **Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.**
Operating Channel	This displays the channel the MWR222 is currently using.

See the rest of this chapter for information on the other labels in this screen.

9.5 Security

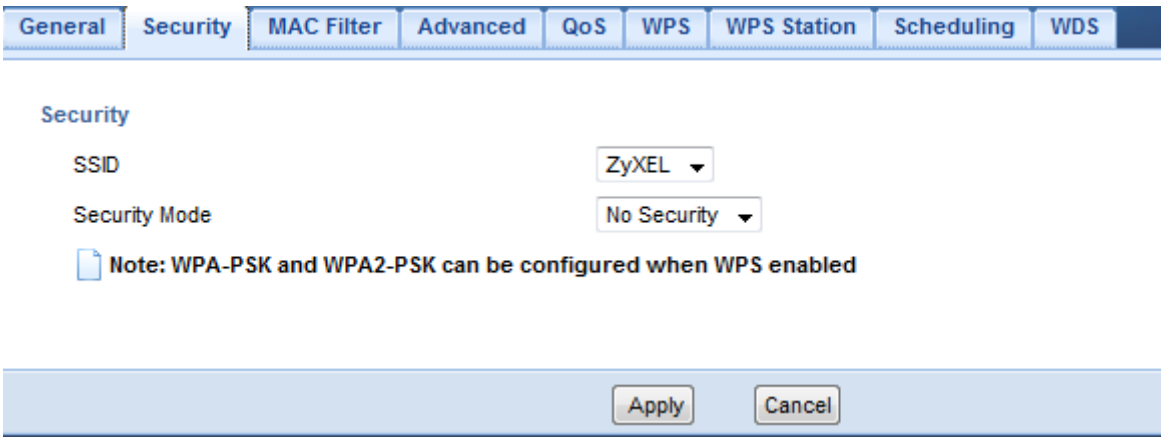
9.5.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your MWR222, your network is accessible to any wireless networking device that is within range.

Figure 43 Network > Wireless LAN > Security: No Security

WPA2-PSK has been reworded to WPA-Personal and WPA2-Personal)



The following table describes the labels in this screen.

Table 23 Network > Wireless LAN > Security: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

Refer to **Table 22** Network > Wireless LAN > General for descriptions of the other labels in this screen.

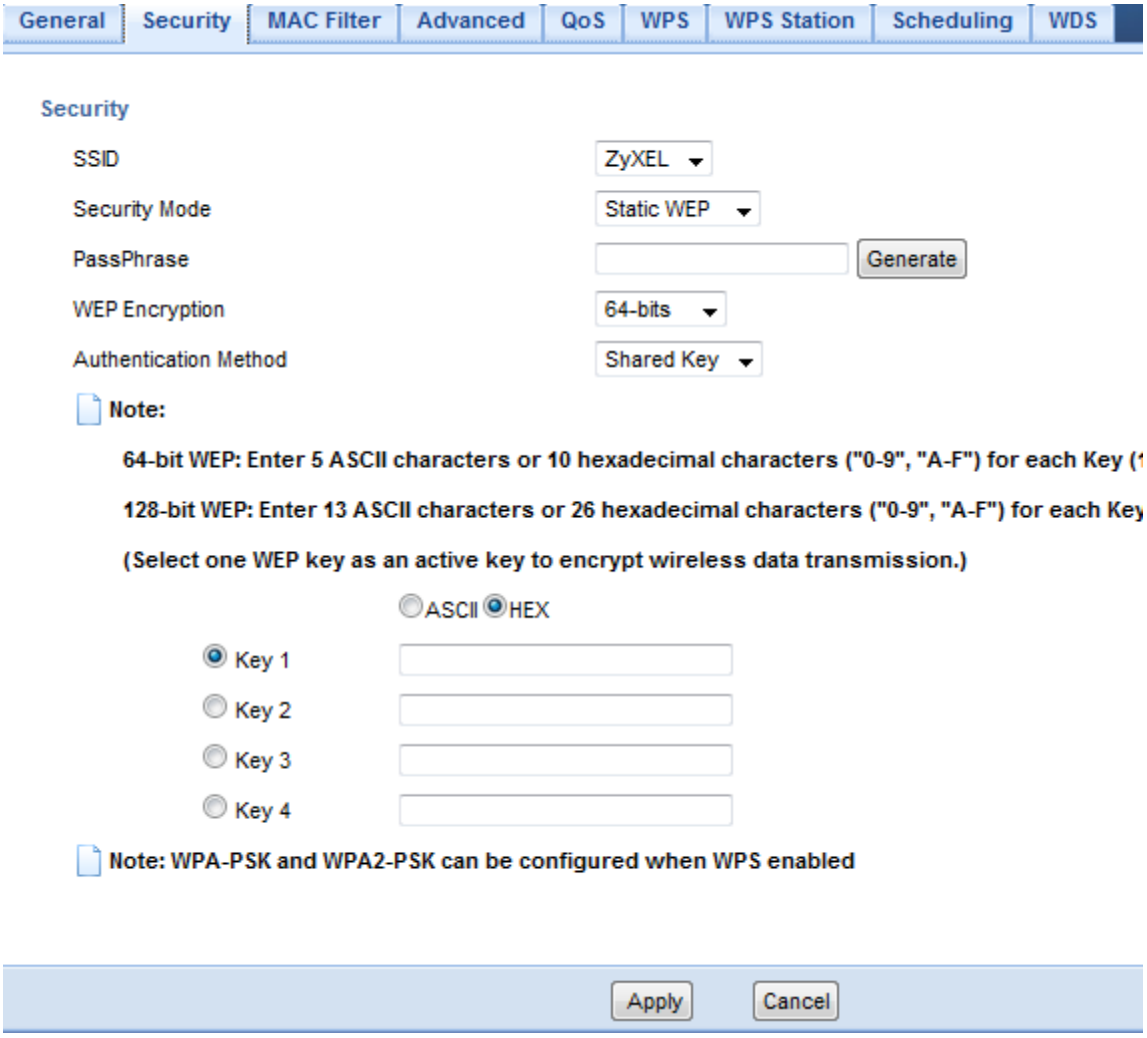
9.5.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your MWR222 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption, click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 44 Network > Wireless LAN > Security: Static WEP



The following table describes the wireless LAN security labels in this screen.

Table 24 Network > Wireless LAN > Security: Static WEP

LABEL	DESCRIPTION
Security Mode	Select **Static WEP** to enable data encryption.
Passphrase	Enter a Passphrase (up to 26 printable characters) and click Generate. A passphrase functions like a password. In WEP security mode, it is further converted by the MWR222 into a complicated string that is referred to as the “key”. This key is requested from all devices wishing to connect to a wireless network.

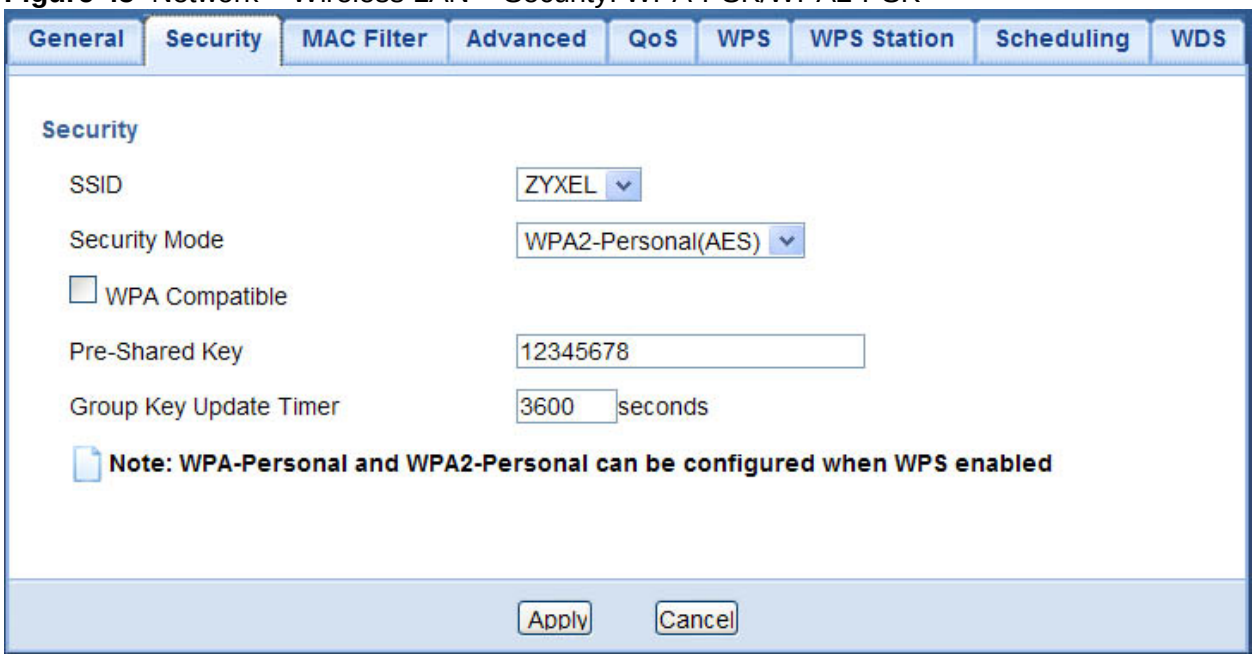
WEP Encryption	Select **64-bit WEP** or **128-bit WEP**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Auto** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the MWR222 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

Refer to **Table 22** Network > Wireless LAN > General for descriptions of the other labels in this screen.

9.5.3 WPA-Personal/Enterprise/WPA2-Personal/Enterprise

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-Persoanl/Enterprise** or **WPA2-Personal/Enterprise** from the **Security Mode** list.

Figure 45 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 25 Network > Wireless LAN > Security: WPA-Personal/Enterprise/WPA2-Persional/Enterprise

LABEL	DESCRIPTION
Security Mode	Select **WPA-Personal / Enterprise** or **WPA2-Personal / Enterprise** to enable data encryption.
WPA-Compatible	This field appears when you choose **WPA2-Personal / Enterprise** as the **Security Mode**. Check this field to allow wireless devices using **WPA-Personal / Enterprise** security mode to connect to your MWR222.
Pre-Shared Key	**WPA-Personal / Enterprise / WPA2-Personal / Enterprise** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the MWR222.

Reset	Click **Reset** to reload the previous configuration for this screen.

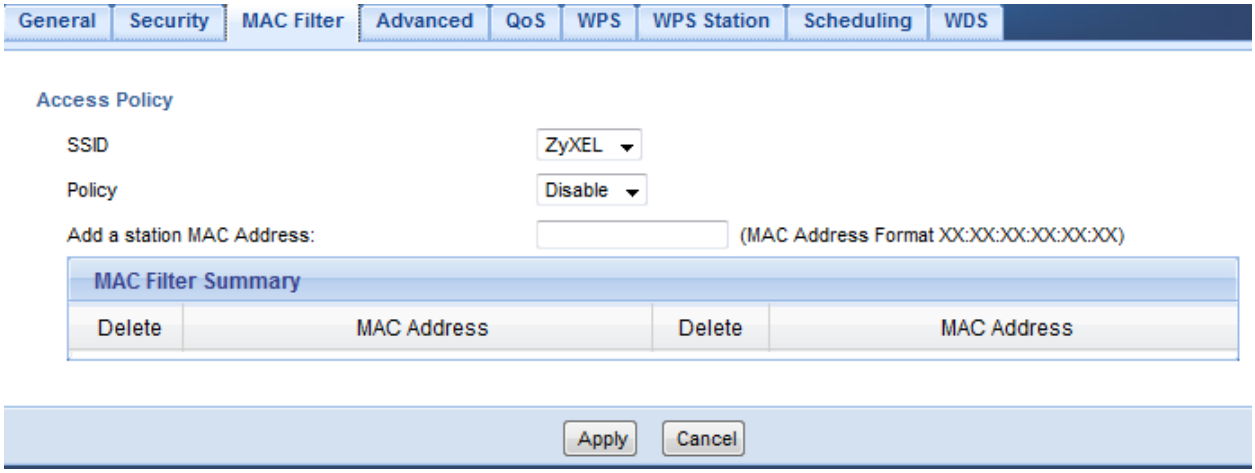
Refer to **Table 22** Network > Wireless LAN > Gener for descriptions of the other labels in this screen.

9.6 MAC Filter

The MAC filter screen allows you to configure the MWR222 to give exclusive access to devices (Allow) or exclude devices from accessing the MWR222 (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your MWR222's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 46 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 26 Network > Wireless LAN > MAC Filter

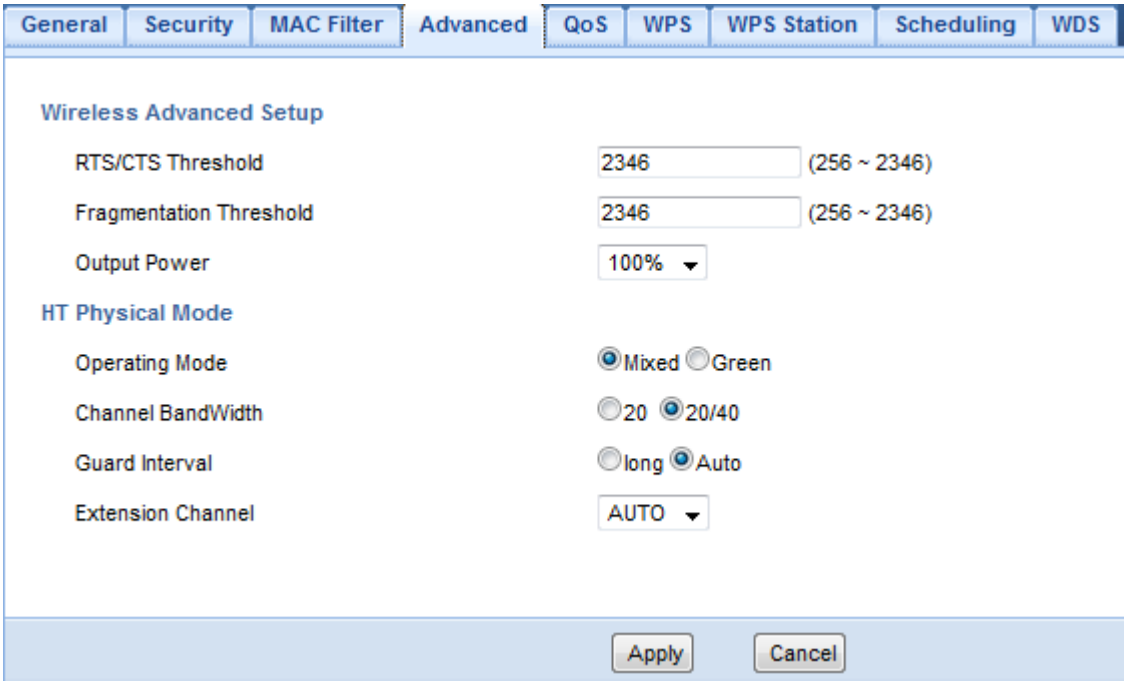
LABEL	DESCRIPTION
Access Policy	
Policy	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Allow** to permit access to the MWR222, MAC addresses not listed will be denied access to the MWR222. Select **Reject** to block access to the MWR222, MAC addresses not listed will be allowed to access the MWR222
Add a station Mac Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the MWR222 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. Click **Add**.
MAC Filter Summary	
Delete	Click the delete icon to remove the MAC address from the list.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the MWR222.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

9.7 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as intra-BSS networking and set the RTS/CTS Threshold

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 47 Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 256 and 2432.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

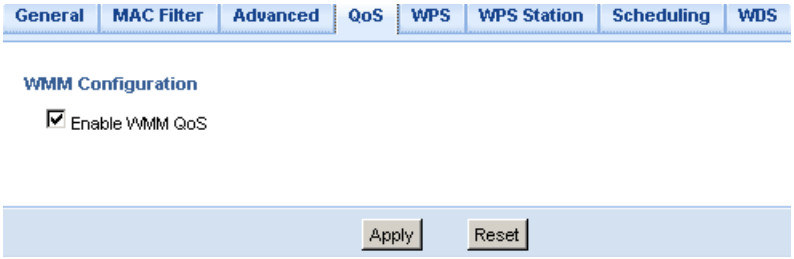
Output Power	Set the output power of the MWR222 in this field. If there is a high density of APs in an area, decrease the output power of the MWR222 to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, 50**%**, **25%**, **10%** or **Minimum**. See the product specifications for more information on your MWR222's output power.
HT (High Throughput) Physical Mode - Use the fields below to configure the 802.11 wireless environment of your MWR222.	
Operating Mode	Choose this according to the wireless mode(s) used in your network. **Mixed Mode** - Select this if the wireless clients in your network use different wireless modes (for example, IEEE 802.11b/g and IEEE 802.1n modes) **Green Mode** - Select this if the wireless clients in your network uses only one type of wireless mode (for example, IEEEE 802.11 n only)
Channel Bandwidth	Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40** (20/40 MHz). Select 20 MHz if you find you have wireless connectivity issues. Using the larger channel bandwidth of 20/40 allows for the possibility of more interference. Use 20 if you have problems connecting from a normal distance wirelessly.
Guard Interval	Select **Auto** to increase data throughput. However, this may make data transfer more prone to errors. Select **Long** to prioritize data integrity. This may be because your wireless network is busy and congested or the MWR222 is located in an environment prone to radio interference.
Extension Channel	This is set to **Auto** by default. If you select **20/40** as your **Channel Bandwidth**, the extension channel enables the MWR222 to get higher data throughput. This also lowers radio interference and traffic.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

9.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

Click **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 48 Network > Wireless LAN > QoS



The following table describes the labels in this screen.

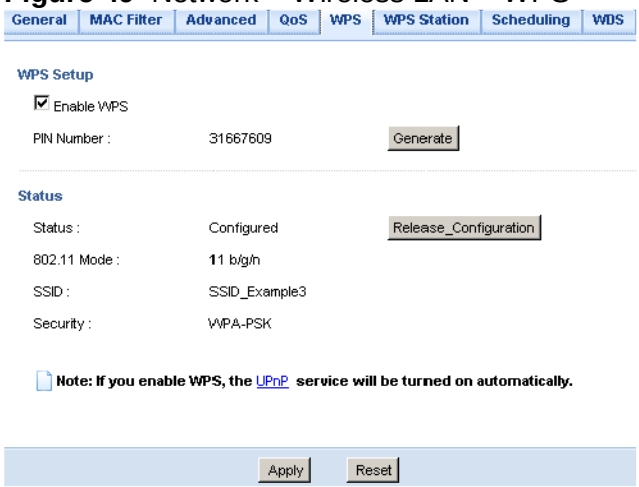
Table 28 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
Enable WMM QoS	Check this to have the MWR222 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click **Apply** to save your changes to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

9.9 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Figure 49 Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > WPS

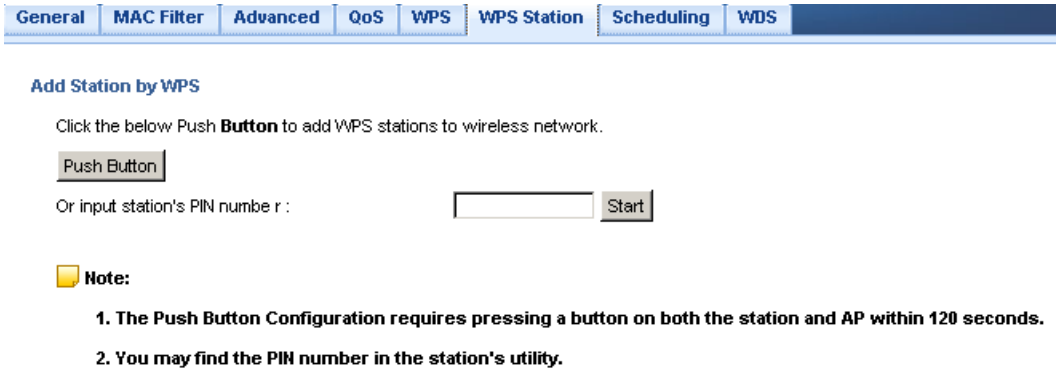
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
Status	
Status	This displays **Configured** when the MWR222 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the MWR222 or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the MWR222.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the MWR222.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes back to the MWR222.
Refresh	Click **Refresh** to get this screen information afresh.

9.10 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 50 Network > Wireless LAN > WPS Station


General
MAC Filter
Advanced
QoS
WPS
WPS Station
Scheduling
WDS
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push Button
Or input station's PIN numbe r :
Start
Note:
1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

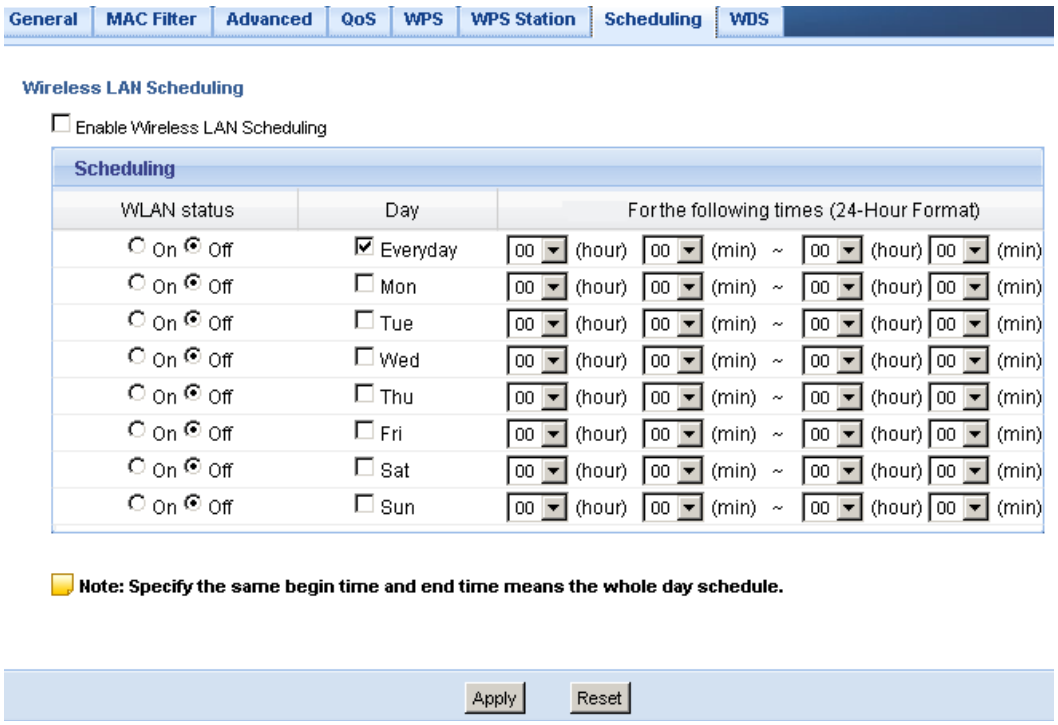
Table 30 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless station's wireless settings. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

9.11 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 51 Network > Wireless LAN > Scheduling



The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Scheduling	
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.

Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you cannot select any specific days. This field works in conjunction with the **Except for the following times** field.
For the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to reload the previous configuration for this screen.

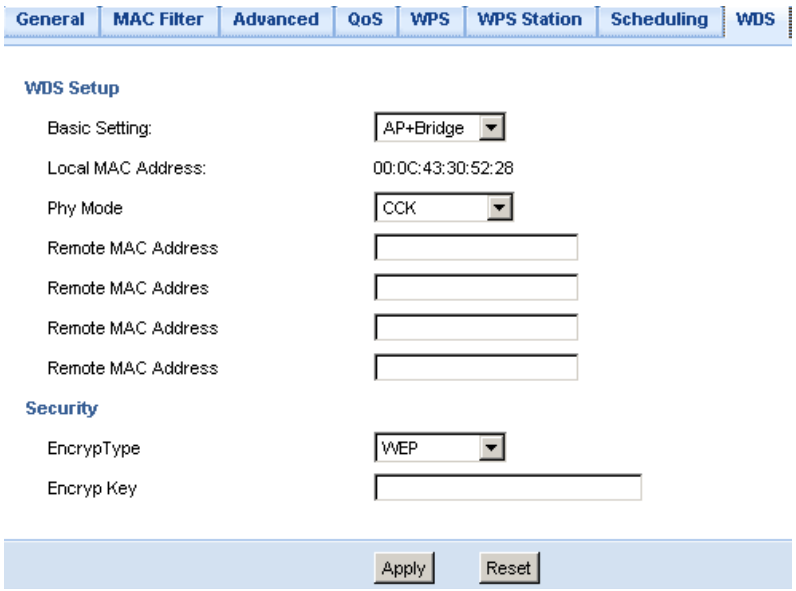
9.12 WDS Screen

A Wireless Distribution System is a wireless connection between two or more APs. Use this screen to set the operating mode of your MWR222 to **AP + Bridge** or **Bridge Only** and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Note: You must enable the same wireless security settings on the MWR222 and on all wireless clients that you want to associate with it.

Click **Network** > **Wireless LAN** > **WDS** tab. The following screen opens with the **Basic Setting** set to **Disabled**, and **Security Mode** set to **No Security**.

Figure 52 Network > Wireless LAN > WDS



The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Settings	Select the operating mode for your MWR222. • **AP + Bridge -** The MWR222 functions as a bridge and access point simultaneously. • **Bridge** - The MWR222 acts as a wireless network bridge. It establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The MWR222 can establish up to five wireless links with other APs.
Local MAC Address	This is the MAC address of your MWR222.
Phy Mode	Select the Phy mode you want the MWR222 to use. This dictates the maximum size of packets during data transmission.
Remote MAC Address	This is the MAC address of the peer device that your MWR222 wants to make a bridge connection with. You can connect to up to 4 peer devices.
Security	
EncrypType	Select whether to use **WEP**, **TKIP** or **AES** encryption for your WDS connection in this field. Otherwise, select **No Security**.
EncrypKey	The Encryp key is used to encrypt data. Peers must use the same key for data transmission.
Apply	Click **Apply** to save your changes to MWR222.
Refresh	Click **Refresh** to reload the previous configuration for this screen.

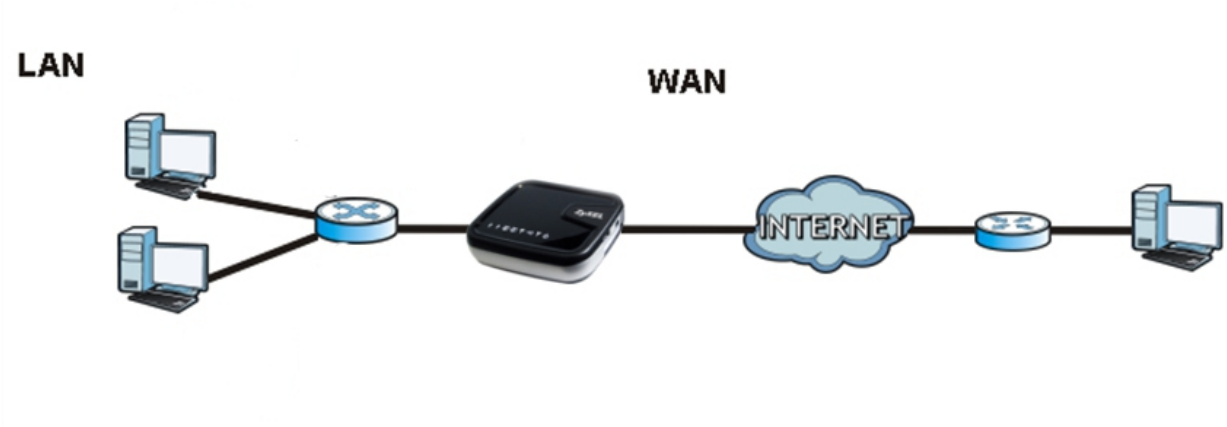
10 WAN

10.1 Overview

This chapter discusses the MWR222's **WAN** screens. Use these screens to configure your MWR222 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 53 LAN and WAN



The MWR222 has two different types of WAN connection. The standard Ethernet WAN connections and the USB port for a 3G adapter.

The standard Ethernet WAN connection is the port labeled "LAN" on the back of the router. The user needs to configure the Ethernet port to WAN to make it to work.

Figure 54 Ethernet and USB Ports

The 3G WAN connection uses wireless 3G adapters connected to a USB port on the MWR222. The USB port is located on the back of the MWR222.

10.2 What You Can Do

- Use the Internet Connection screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC Address
- Use the **Advanced** screen to enable multicasting, configure Windows networking and bridge.
- Use **IGMP Snooping** screen to enable IGMP snooping in the LAN ports.

10.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your MWR222.

10.3.1 Configuring Your Internet Connection

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the MWR222, which makes it accessible from an outside network. It is used by the MWR222 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the MWR222 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The MWR222 can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2. If your ISP dynamically assigns the DNS server IP addresses (along with the MWR222's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

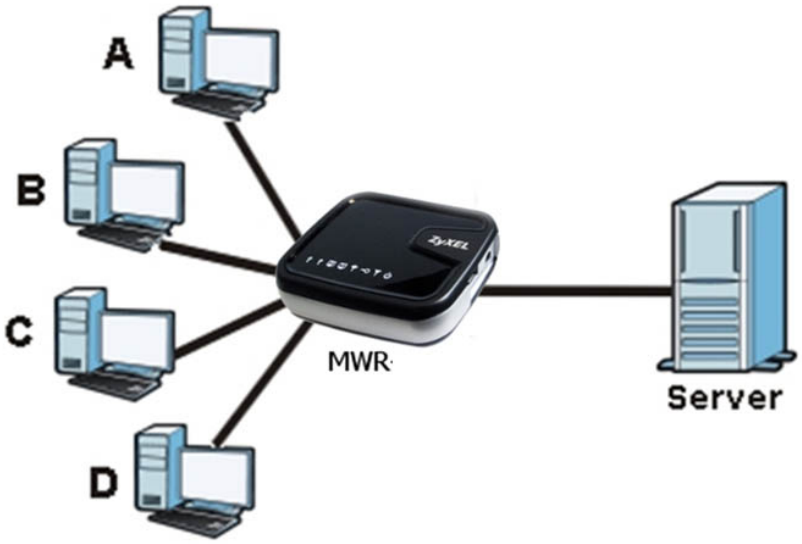
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

10.3.2 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (one sender - one recipient) or Broadcast (one sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one. Multicast is a function that lowers bandwidth needed to stream media to multiple recipients. Rather than sending a stream for each computer connected with multicast, one stream is sent and when it reaches its final routing point the information splits and is sent to all subscribed multicast connections.

Figure 55 Multicast Example



In the multicast example above, systems A and D comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and D.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The MWR222 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the MWR222 queries all directly connected networks to gather group membership. After that, the MWR222 periodically updates this information. IP multicasting can be enabled/disabled on the MWR222 LAN and/or WAN interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

10.4 Internet Connection

Use this screen to change your MWR222's Internet access settings. Click **WAN** from the Configuration menu. The screen differs according to the encapsulation you choose.

10.4.1 Ethernet Encapsulation

This screen displays when you select **Ethernet** encapsulation.

Figure 56 Network > WAN > Wired WAN: Ethernet Encapsulation

The following table describes the labels in this screen.

Table 33 Network > WAN > Wired WAN: Ethernet Encapsulation

LABEL	DESCRIPTION
Ethernet Port Type	Sets the Ethernet port to function as either LAN or WAN.
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
WAN DNS Assignment	

First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the MWR222's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4.2 PPPoE Encapsulation

The MWR222 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

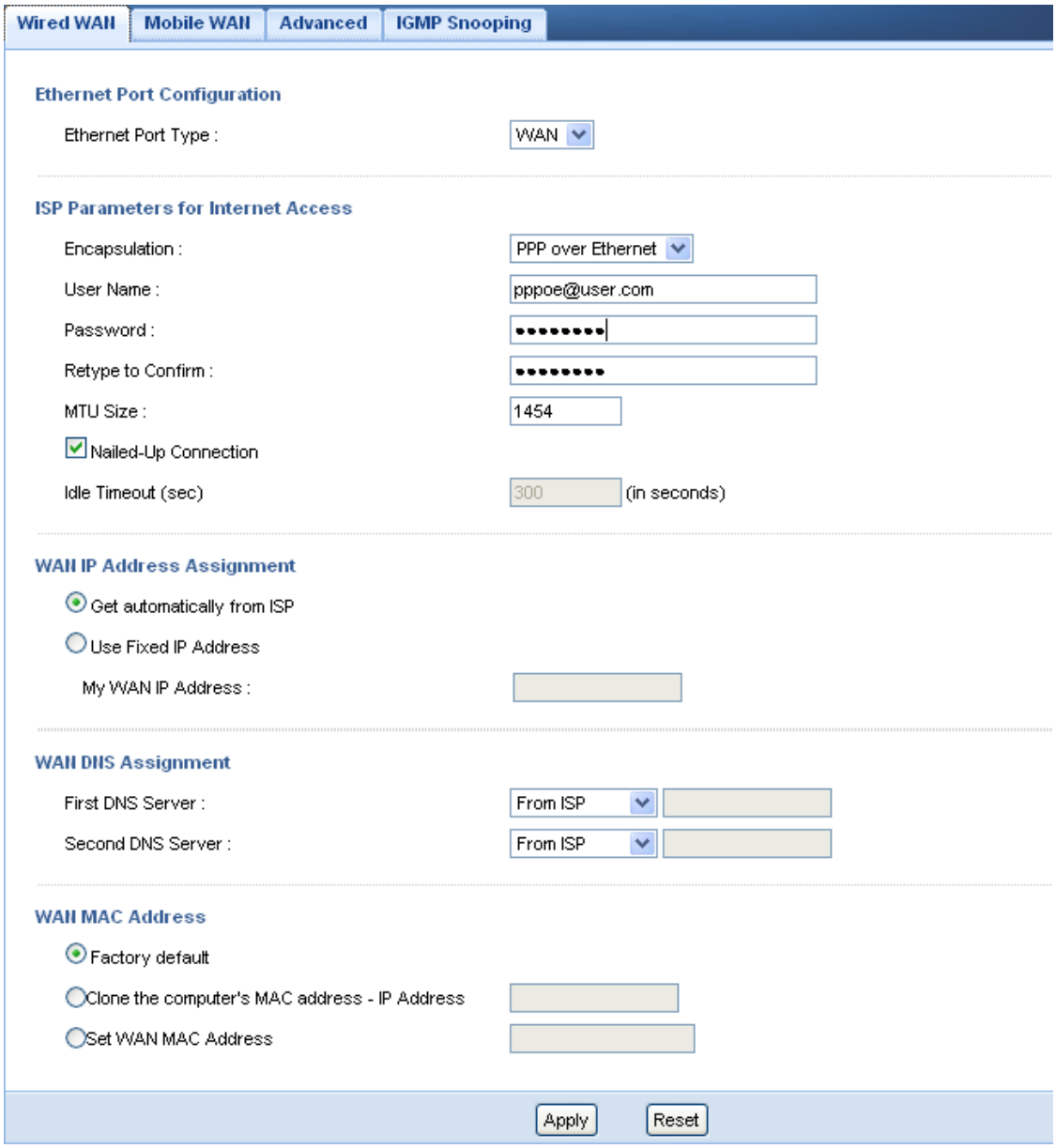
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the MWR222 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the MWR222 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 57 Network > WAN > Wired WAN: PPPoE Encapsulation



The following table describes the labels in this screen.

Table 34 Network > WAN > Wired WAN: PPPoE Encapsulation

LABEL	DESCRIPTION
Ethernet Port Configuration	
Ethernet Port Type	Select WAN when using the Ethernet port for WAN configuration
ISP Parameters for Internet Access	
Encapsulation	Select **PPP over Ethernet** if you connect to your Internet via dial-up.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your MWR222 can receive and process.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout (sec)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.

WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the MWR222's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

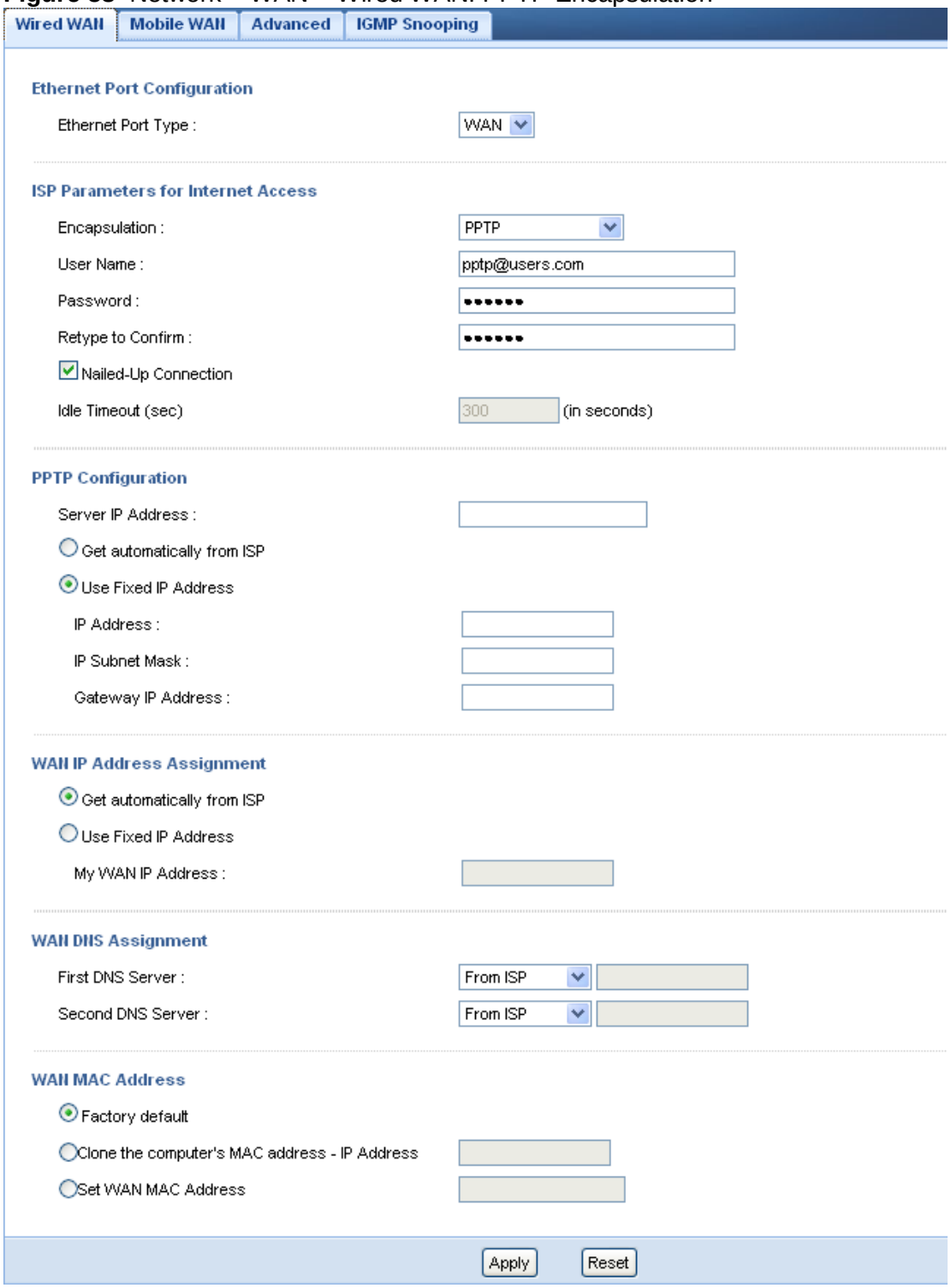
10.4.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

This screen displays when you select **PPTP** encapsulation.

Figure 58 Network > WAN > Wired WAN: PPTP Encapsulation



The following table describes the labels in this screen.

Table 35 Network > WAN > Wired WAN: PPTP Encapsulation

LABEL	DESCRIPTION
Ethernet Port Configuration	
Ethernet Port Type	Select WAN when using the Ethernet port for WAN configuration
ISP Parameters for Internet Access	
Connection Type	To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the MWR222 automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.

IP Subnet Mask	Your MWR222 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the MWR222.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the MWR222's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.

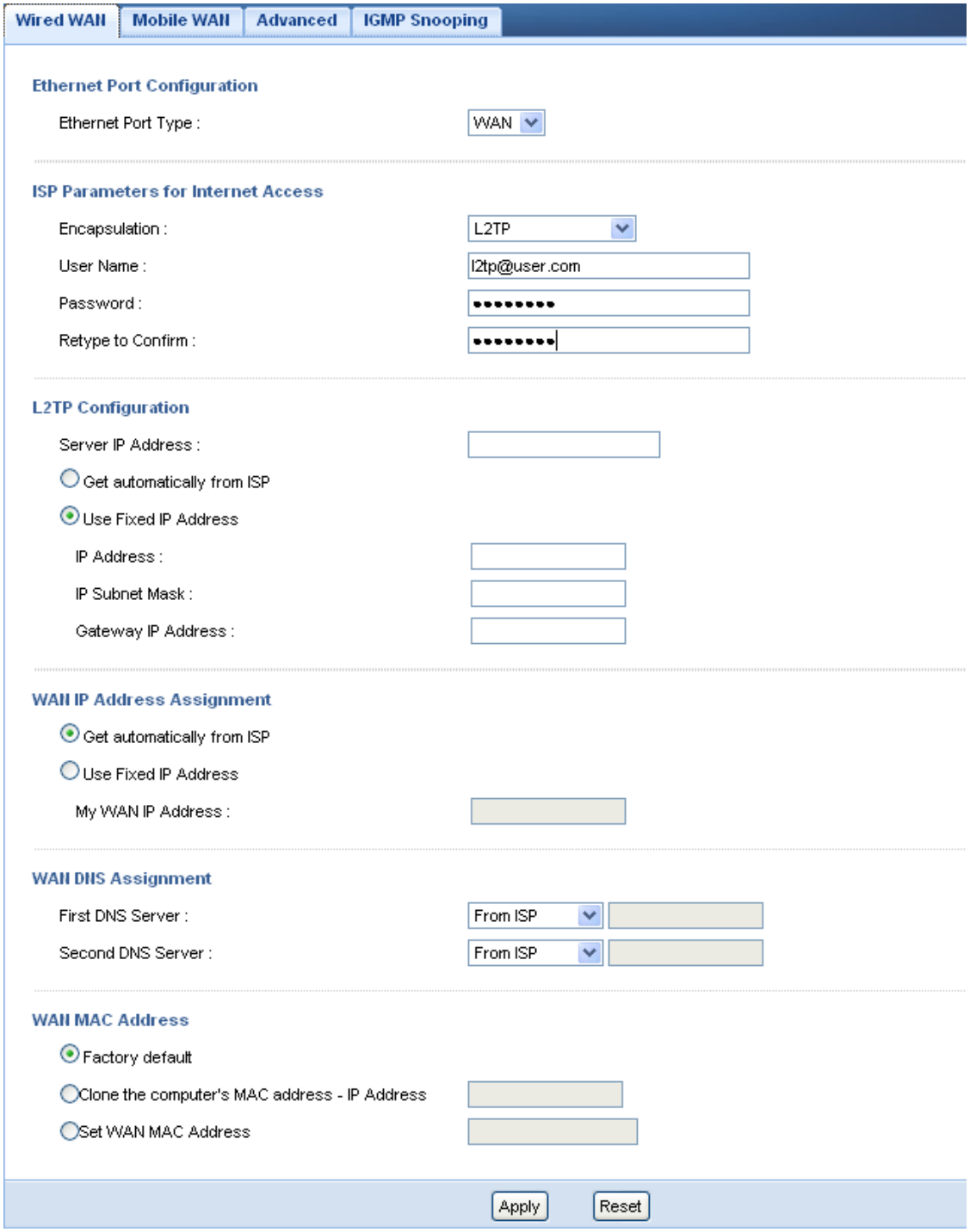
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4.4 L2TP Encapsulation

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peer devices over another network (like the Internet).

This screen displays when you select **L2TP** encapsulation.

Figure 59 Network > WAN > Wired WAN: L2TP Encapsulation



The following table describes the labels in this screen.

Table 36 Network > WAN > Wired WAN: L2TP Encapsulation

LABEL	DESCRIPTION
Ethernet Port Configuration	
Ethernet Port Type	Select WAN when using the Ethernet port for WAN configuration
ISP Parameters for Internet Access	
Connection Type	To configure a L2TP client, you must configure the **User Name** and **Password** fields for a layer-2 connection and the L2TP parameters for an L2TP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
L2TP Configuration	
Server IP Address	Type the IP address of the L2TP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Your MWR222 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the MWR222.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.

WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the MWR222's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

10.5 Mobile WAN

The Mobile WAN connection uses a broadband 3G connection via USB adapter provided by a mobile broadband ISP. This allows for mobile connection to the internet within the 3G coverage of your selected mobile provider.

This screen displays when you select the **Mobile WAN** tab.

Figure 60(a) Network > WAN > Mobile WAN > WiMAX Only

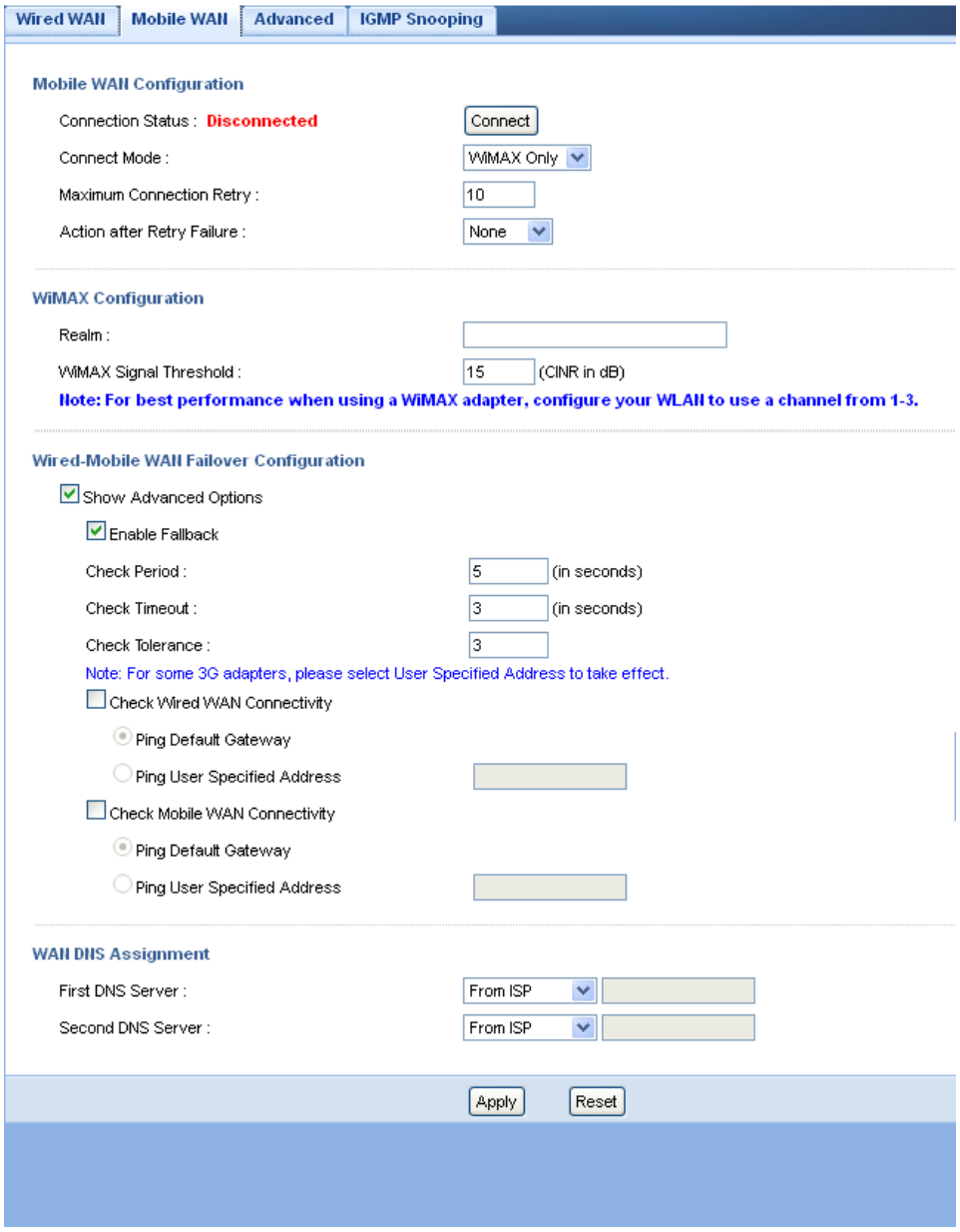


Figure 60(b) Network > WAN > Mobile WAN > Verizon LTE

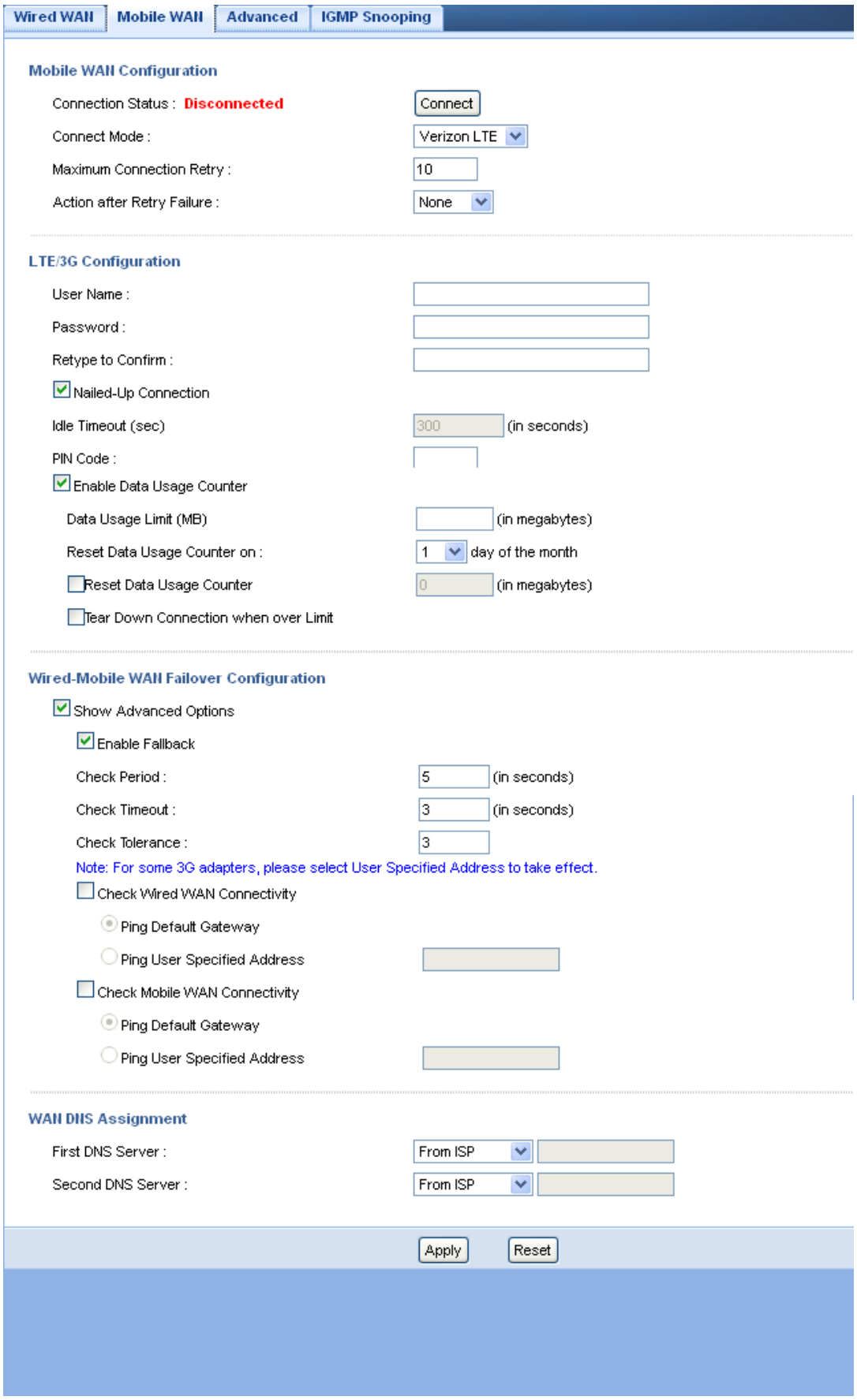
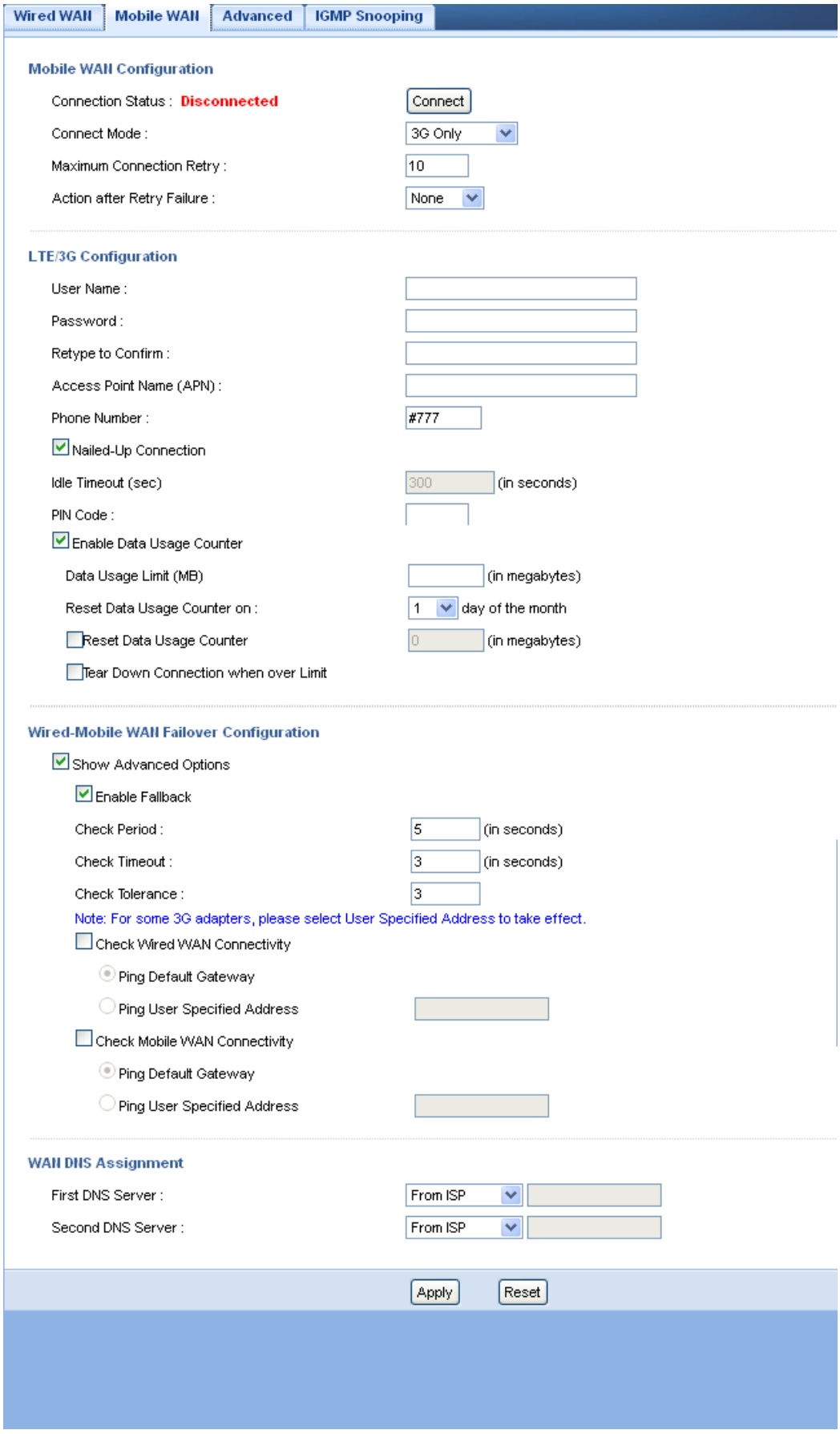


Figure 60(c) Network > WAN > Mobile WAN > 3G Only



The following table describes the labels in this screen.

Table 37 Network > WAN > Mobile WAN

LABEL	DESCRIPTION
Mobile WAN Configuration	
Connection Status	Once your connection setting shave been applied, click the Connect button to connect your Mobile WAN. When the Status says Disconnected, the Mobile WAN is not connected. When it says Connected, it has successfully established a connection.
Connection Mode	Choose **Auto** for an automatic detection of wireless WAN type. The MWR will first try to establish an WiMAX connection before trying to establish a 3G connection. Auto mode does not support LTE connection.
Min. WiMAX signal Threshold	Min. WiMAX Signal Threshold is the minimum CINR value the MWR will allow before determining dropping the WiMAX signal.
Enables 3G to WiMAX reconnect	MWR will try to reconnect to WiMAX network whenever a WiMAX network is detected while a 3G connection has been established.
Check Period (second)	This is the value for how often the MWR will check for available WiMAX signal. The default value is 180 in seconds.
Maximum Connection Retry	This is the value MWR will try to connect to WiMAX or 3G before giving up.
Action After Retry	There are three options for the MWR to take after failure to establish connections even after retry. **None** for do nothing, **Reboot** for rebooting the MWR and **Wait** for other commands.

Failure	
WiMAX Configuration	
Realm	Enter this field accordingly provided by your ISP. In most cases, it can be left blank unless ISP notices otherwise.
WiMAX Signal Threshold	WiMAX signal threshold marked with CINR in dB, which stands for "Carrier Interferrence and Noise Ratio." MWR detects CINR when it tries to connect to a WiMAX base station. The value is default at "15" and is better when its higher.
LTE/3G Configuration	
Username	Type the user name given to you by your mobile provider. (not all ISP needs this)
Password	Type the password associated with the User Name above. (not all ISP needs this)
Retype to Confirm	Type your password again to make sure that you have enter the password correctly.
Access Point Name	
Phone Number	
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout (sec)	This value specifies the time in minutes that elapses before the MWR222 automatically disconnects from the mobile connection.
PIN Code	Type the Pin Code given to you by your mobile broadband provider.
Enable Data Usage Counter	Select this option to enable the Data Usage Counter settings. The data usage counter is for user convenience. It is not synchronized with the Carrier's actual data usage.

Data Usage Limit (MB)	Enter the desired data usage limit in megabytes. Example: 5 gigabytes equals 5000 megabytes.
Reset Data Usage Counter On	Select the day of the month for the Data Usage Counter Reset to the default value.
Reset Data Usage counter	Select the value in megabytes for the Data Usage Counter to begin counting from. Example: You have 100Mb of data usage available but you do not want to allow the entire 100Mb to be used. You can set the Reset Data Usage Counter to 60Mb and the Data Usage Counter will start at 60Mb. When the Data Usage Limit reaches 100Mb, you will still have 40Mb left from the total 100Mb. This will allow you to be notified when close to your Data Usage Limit and not when it has been fully emptied.
Tear Down Connection when over Limit	Select this option to automatically disconnect your mobile broadband connection when you reach your Data Usage limit.
Wired-Mobile WAN Failover Configuration	
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
LABEL	**DESCRIPTION**

ISP Parameters for Internet Access	
Connection Status	Once your connection settings have been applied, click the Connect button to connect your Mobile WAN. When the Status says Disconnected the Mobile WAN is not connected. When it says Connected it has successfully connected.
User Name	Type the user name given to you by your mobile provider. (not all ISP needs this)
Password	Type the password associated with the User Name above. (not all ISP needs this)
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Access Point Name (APN)	Type the name of the access point provided to you by the mobile broadband provider. (not all ISP needs this)
Phone Number	Type the phone number provided by your mobile broadband provider. The default phone number is #777 (for CDMA carriers such as Sprint or Verizon). If the phone number is left as blank, MWR222 will implicitly use #777 to connect.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the MWR222 automatically disconnects from the mobile connection.
Mobile WAN Configuration	
USB Mobile WAN Adapter	Select your mobile broadband provider's USB adapter from the list or select **Auto-detect** to let the MWR222 find yours automatically.
Pin Code	Type the Pin Code given to you by your mobile broadband provider.
Enable Data Usage Counter	Select this option to enable the Data Usage Counter settings. The data usage counter is for user convenience. It is not synchronized with the Carrier's actual data usage.
Data Usage Limit (Mb)	Enter the desired data usage limit in megabytes. Example: 5 gigabytes equals 5000 megabytes.

Reset Data Usage Counter on	Select the day of the month for the Data Usage Counter Reset to the default value.
Reset Data Usage Counter	Select the value in megabytes for the Data Usage Counter to begin counting from. Example: You have 100Mb of data usage available but you do not want to allow the entire 100Mb to be used. You can set the Reset Data Usage Counter to 60Mb and the Data Usage Counter will start at 60Mb. When the Data Usage Limit reaches 100Mb, you will still have 40Mb left from the total 100Mb. This will allow you to be notified when close to your Data Usage Limit and not when it has been fully emptied.
Tear Down Connection when over Limit	Select this option to automatically disconnect your mobile broadband connection when you reach your Data Usage limit.
Failover Configuration	
Enable Fallback	Select this option to have the MWR222 return to wired WAN if it is available.
Check Period	The interval to wait when monitoring the wired WAN and mobile WAN connections. The shorter the time period, the faster the MWR will react to an interruption in one of the WAN connections, but the more network bandwidth is used (if connectivity check enabled) and the more system resources are used.
Check Timeout	If connectivity check is enabled, how long to wait for a reply from a remote host before counting it as a failure.
Check Tolerance	If connectivity check is enabled, how many consecutive failures are needed before the connection is considered broken.
Check Wired WAN Connectivity	Select this option to have the MWR222 ping a remote host to determine if the wired WAN connection is alive. Using a connectivity check consumes a minimal amount of network bandwidth but allows the MWR222 to detect network unavailability caused by an upstream interruption. Without connectivity check the MWR can only monitor the direct physical link.
Ping Default Gateway	If connectivity check is enabled, the remote host to monitor. This can either be the gateway of the WAN interface.\ Note: certain mobile WAN providers do not allow the gateway to reply to pings, so using that option for mobile WAN may produce false negatives.

Ping User Specified Address	If the ping target is set to user specified address, the specific IP address to monitor.
Check Wired WAN Connectivity	Select this option to have the MWR222 ping a remote host to determine if the wired WAN connection is alive. Using a connectivity check consumes a minimal amount of network bandwidth but allows the MWR222 to detect network unavailability caused by an upstream interruption. Without connectivity check the MWR can only monitor the direct physical link.
Ping Default Gateway	If connectivity check is enabled, the remote host to monitor. This can either be the gateway of the WAN interface Note: certain mobile WAN providers do not allow the gateway to reply to pings, so using that option for mobile WAN may produce false negatives.
Ping User Specified Address	If the ping target is set to user specified address, the specific IP address to monitor.
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the MWR222's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.

Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Connect	Click **Connect** to save your changes back to the MWR222. If a 3G adapter is inserted in the USB port, MWR222 will start connection.
Reset	Click **Reset** to begin configuring this screen afresh.

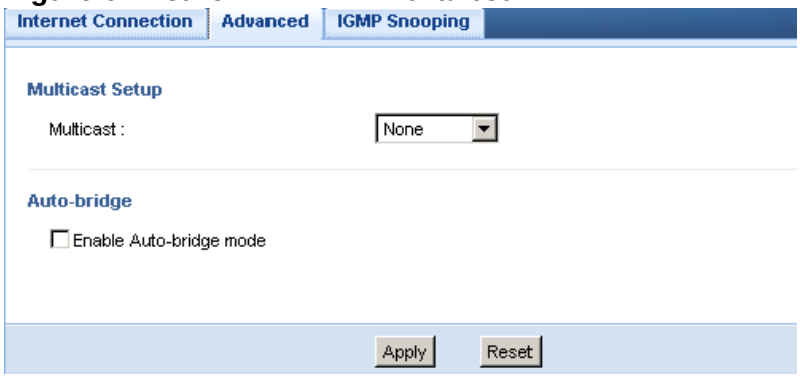
10.6 Advanced WAN Screen

Use this screen to enable **Multicast** and enable **Auto-bridge**.

Note: The categories shown in this screen are independent of each other.

To change your MWR222's advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 61 Network > WAN > Advanced



The following table describes the labels in this screen.

Table 38 Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select **IGMPv1/v2** to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select **None** to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
Auto-bridge	

Enable Auto-bridge mode	Select this option to have the MWR222 switch to bridge mode automatically when the MWR222 gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

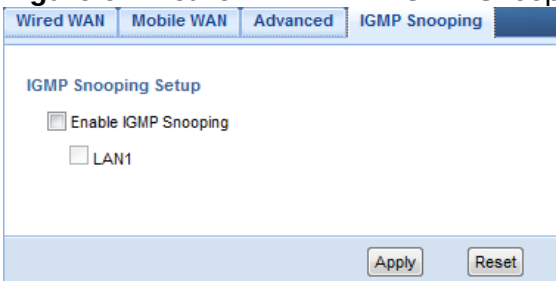
10.7 IGMP Snooping Screen

Use this screen to enable IGMP snooping if you have LAN users that subscribe to multicast services.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data.

Click **Network > WAN > IGMP Snooping**. The screen appears as shown.

Figure 62 Network > WAN > IGMP Snooping



The following table describes the labels in this screen.

Table 39 Network > WAN > IGMP Snooping

LABEL	DESCRIPTION
Auto-bridge	
Enable IGMP Snooping	Select this option to have the MWR222 use IGMP snooping. Check the LAN port to which IGMP snooping applies.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

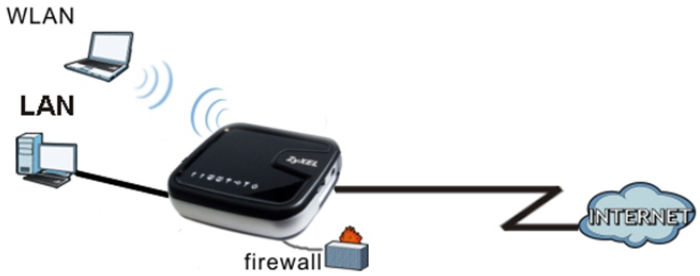
11 LAN

11.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Figure 63 LAN Example (implies wired WAN connection)



The LAN screens can help you manage IP addresses.

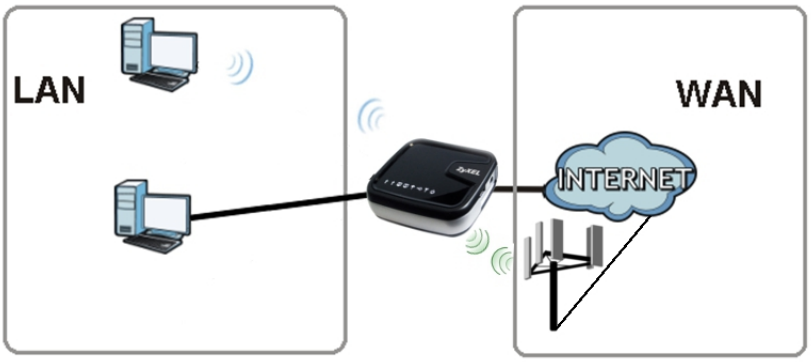
11.2 What You Can Do

- Use the **IP** screen to change the IP address for your MWR222.
- Use the **IP Alias** screen to have the MWR222 apply IP alias to create LAN subnets.

11.3 What You Need To Know

The actual physical connection determines whether the MWR222 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 64 LAN and WAN IP Addresses (implies wired WAN connection)



The LAN parameters of the MWR222 are preset in the factory with the following values:

- IP address of 192.168.10.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.10.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

11.3.1 IP Pool Setup

The MWR222 is pre-configured with a pool of 32 IP addresses starting from 192.168.10.33 to 192.168.10.64. This configuration leaves 31 IP addresses (excluding the MWR222 itself) in the lower range (192.168.10.2 to 192.168.10.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

11.3.2 LAN TCP/IP

The MWR222 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

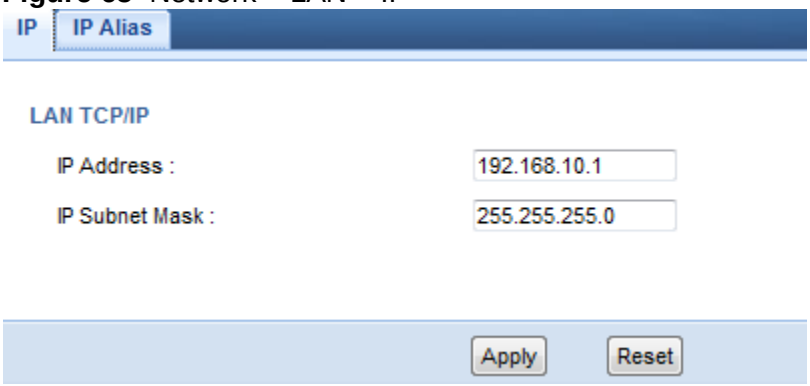
11.3.3 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The MWR222 supports three logical LAN interfaces via its single physical Ethernet interface with the MWR222 itself as the gateway for each LAN network.

11.4 LAN IP Screen

Use this screen to change the IP address for your MWR222. Click **Network > LAN > IP**.

Figure 65 Network > LAN > IP



The following table describes the labels in this screen.

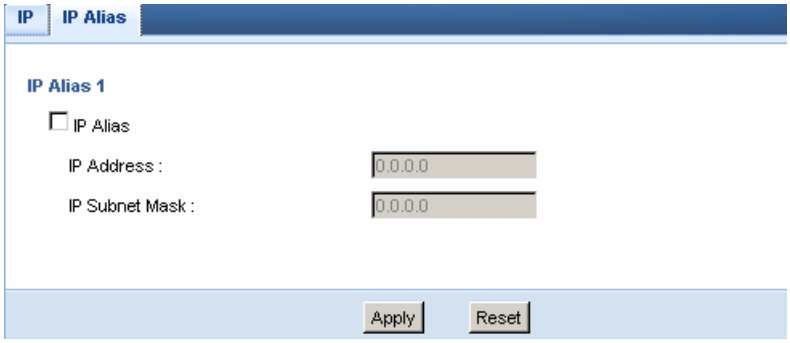
Table 40 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your MWR222 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your MWR222 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the MWR222.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 IP Alias Screen

Use this screen to have the MWR222 apply IP alias to create LAN subnets. Click **LAN > IP Alias**.

Figure 66 Network > LAN > IP Alias



The following table describes the labels in this screen.

Table 41 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Check this to enable IP alias.
IP Address	Type the IP alias address of your MWR222 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your MWR222 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the MWR222.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

12 DHCP Server

12.1 Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the MWR222's LAN as a DHCP server or disable it. When configured as a server, the MWR222 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

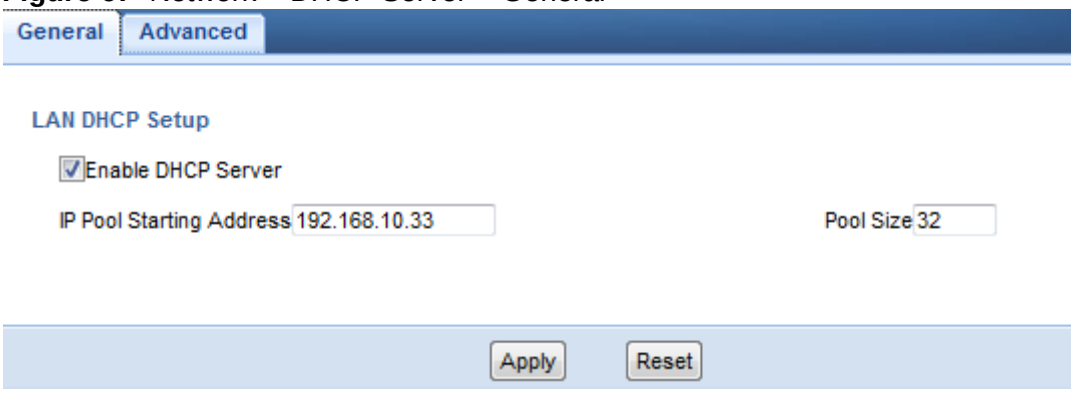
12.2 What You Can Do

- Use the **General** screen to enable the DHCP server.
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

12.3 General Screen

Use this screen to enable the DHCP server. Click **Network** > **DHCP Server**. The following screen displays.

Figure 67 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 42 Network > DHCP Server > General

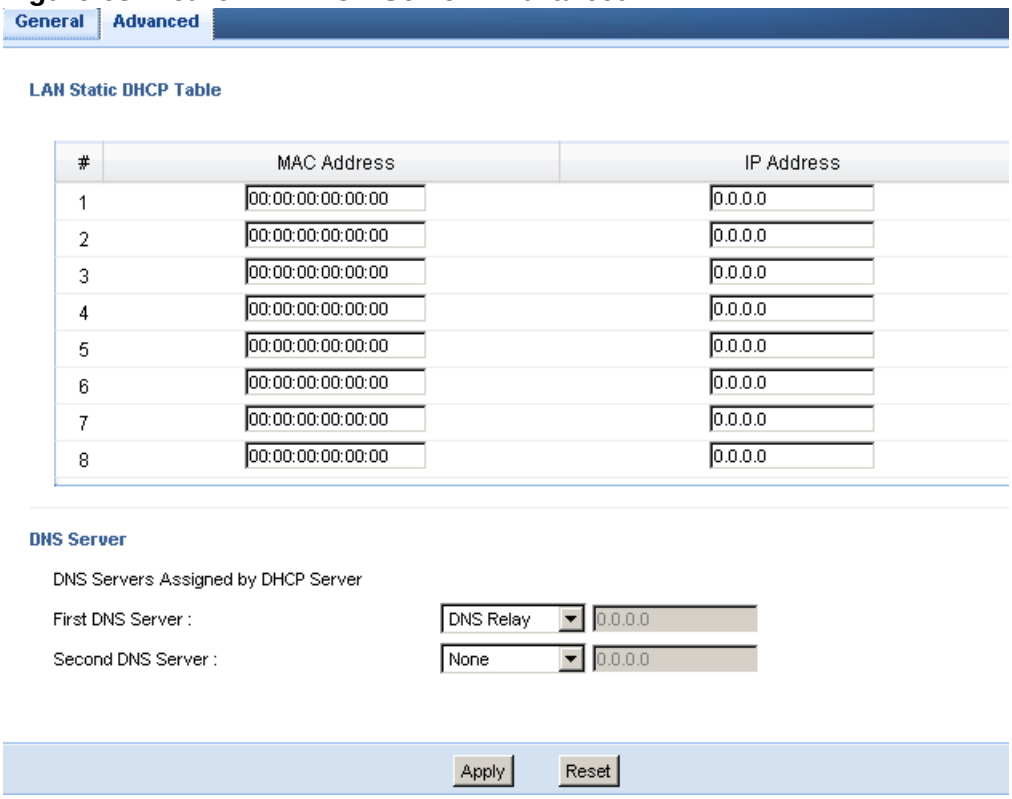
LABEL	DESCRIPTION
Enable DHCP Server	Enable or Disable DHCP for LAN.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

12.4 Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the MWR222 sends to the DHCP clients.

To change your MWR222's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 68 Network > DHCP Server > Advanced



The following table describes the labels in this screen.

Table 43 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
LAN Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The MWR222 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The MWR222 only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the MWR222's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the MWR222 act as a DNS proxy. The MWR222's LAN IP address displays in the field to the right (read-only). The MWR222 tells the DHCP clients on the LAN that the MWR222 itself is the DNS server. When a computer on the LAN sends a DNS query to the MWR222, the MWR222 forwards the query to the MWR222's system DNS server (configured in the **WAN > Internet Connection** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

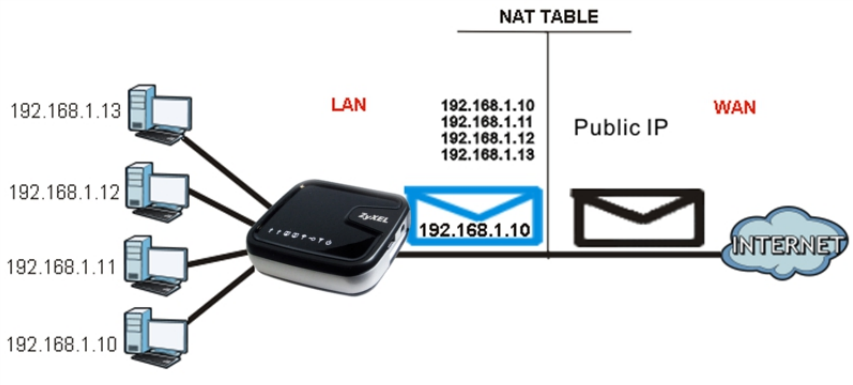
13. Network Address Translation (NAT)

13.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

Each packet has two addresses – a source address and a destination address. For outgoing packets, NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The MWR222 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 69 NAT Example (use 192.168.10.x to be consistent with default value)



For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

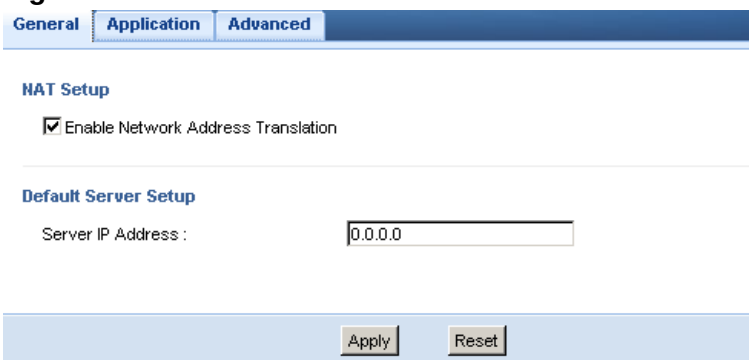
13.2 What You Can Do

- Use the **General** screen to enable NAT and set a default server.
- Use the **Application** screen to forward incoming service requests to the server(s) on your local network.
- Use the **Advanced** screen to change your MWR222's trigger port settings.

13.3 General NAT Screen

Use this screen to enable NAT and set a default server. Click **Network > NAT > General** to open the following screen.

Figure 70 Network > NAT > General



The following table describes the labels in this screen.

Table 44 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Default Server Setup	
Server IP Address	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Application** screen. If you do not assign a **Default Server IP address**, the MWR222 discards all packets received for ports that are not specified in the **Application** screen or remote management.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

13.4 NAT Application Screen

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

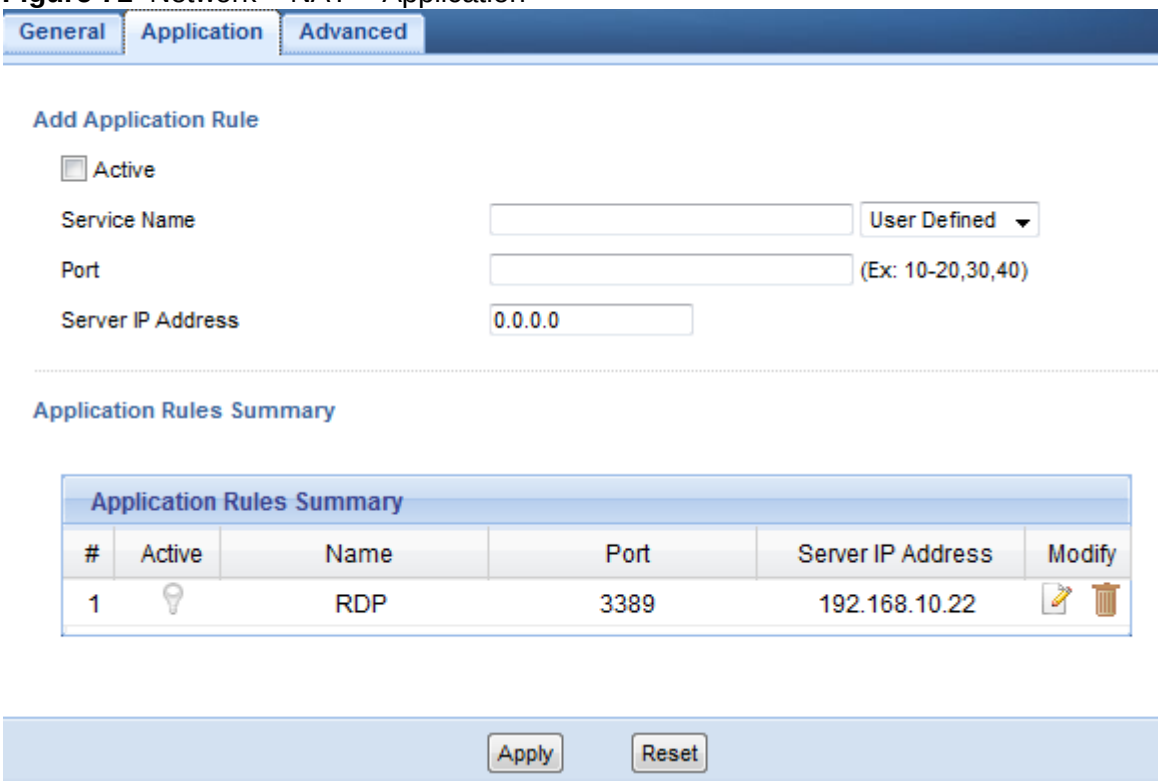
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your MWR222's port forwarding settings, click **Network > NAT** > **Application**. The screen appears as shown.

Note: If you do not assign a **Default Server IP address** in the **NAT > General** screen, the MWR222 discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix E for port numbers commonly used for particular services.

Figure 71 Network > NAT > Application



The following table describes the labels in this screen.

Table 45 Network > NAT > Application

LABEL	DESCRIPTION
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.
Port	Type a port number(s) to define the service to be forwarded to the specified server. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them

	by a comma without spaces, such as 123,567.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the port(s) specified in the **Port** field.
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

13.5 NAT Advanced Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually

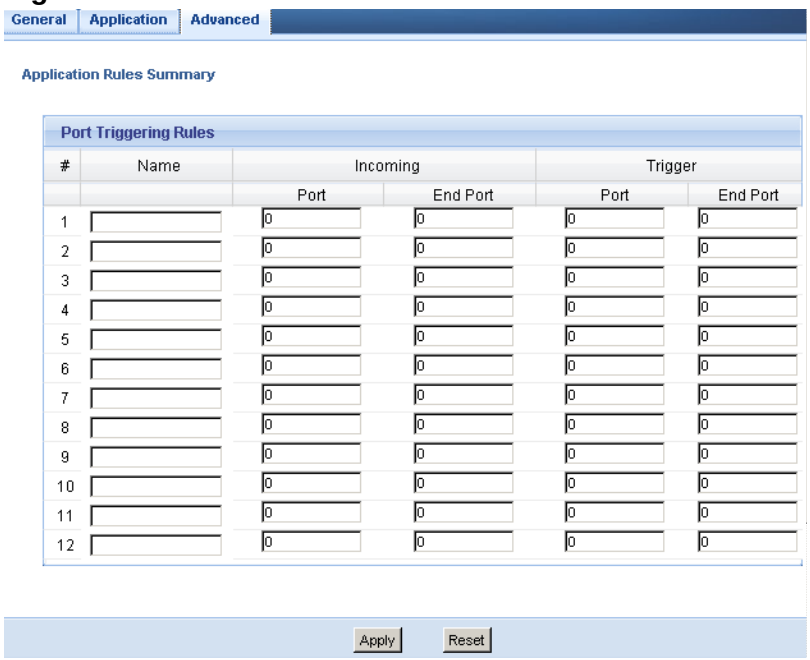
replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The MWR222 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the MWR222's WAN port receives a response with a specific port number and protocol ("incoming" port), the MWR222 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

To change your MWR222's trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 72 Network > NAT > Advanced



The following table describes the labels in this screen.

Table 46 Network > NAT > Advanced

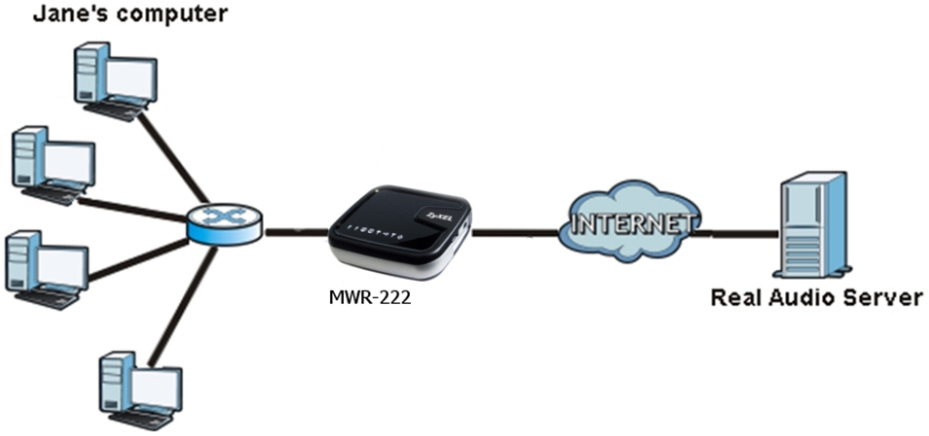
LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes.

	All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The MWR222 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the MWR222 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

13.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 73 Trigger Port Forwarding Process:



Example

1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a “trigger” port and causes the MWR222 to record Jane’s computer IP address. The MWR222 associates Jane's computer IP address with the "incoming" port range of 6970-7170.

3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The MWR222 forwards the traffic to Jane’s computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The MWR222 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

13.5.2 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is going coming from inside the MWR222 and going to the outside.

2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

14 Dynamic DNS

14.1 Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

14.2 What You Can Do

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the MWR222.

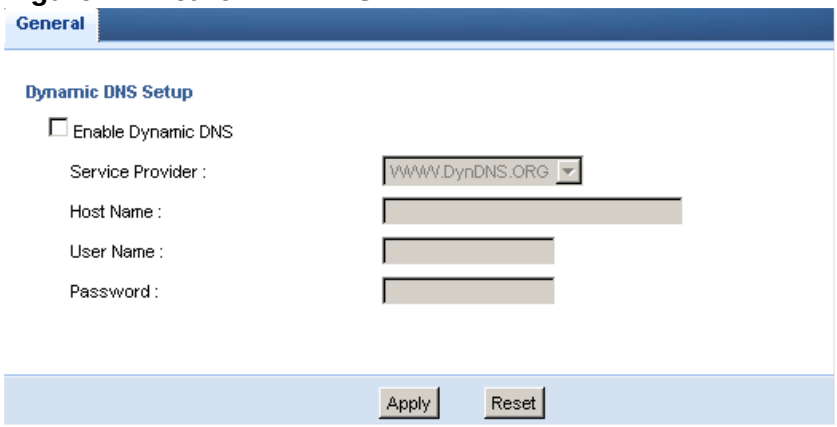
14.3 What You Need To Know

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

14.4 Dynamic DNS Screen

To change your MWR222's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 74 Network > DDNS



The following table describes the labels in this screen.

Table 47 Network > DDNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

15. OpenDNS

15.1 Overview

This chapter shows you how to configure OpenDNS for your MWR222.

OpenDNS is the leading provider of free security and infrastructure services that make the Internet safer through integrated Web content filtering, anti-phishing and DNS. OpenDNS services enable consumers and network administrators to secure their networks from online threats, reduce costs and enforce Internet-use policies. OpenDNS is used today by millions of users and organizations around the world.

http://www.opendns.com

15.2 What you can do

OpenDNS integration in the MWR222 allows you do easily link your OpenDNS account with the MWR222.

(user also need to configure WAN DNS Assignment to OpenDNS)

15.3 OpenDNS Screen

Click **Network** > **OpenDNS** to view the **OpenDNS** screen

Figure 75 Network > OpenDNS

General
OpenDNS Setup
Create New Account / Configure Personalized Setting
Click here to OpenDNS
Note:
After OpenDNS setting is configured via OpenDNS website, please choose OpenDNS specific DNS server under WAN DNS Assigement in WAN page.
Enable OpenDNS
Host Name :
User Name :
Password :
Apply
Reset

The following table describes the labels on this screen.

Table 48 Network > OpenDNS

LABEL	DESCRIPTION
OpenDNS Setup	
Create New Account / Configure Personalized Setting	Use the “Click here to OpenDNS” link to open http://www.opendns.com.
Enable OpenDNS	Select this check box to use OpenDNS after configuring an account on http://www.opendns.com.
Host Name	Type the **Host Name** provided by OpenDNS.
User Name	Type the **User Name** you created with OpenDNS.
Password	Type the **Password** tied to the User Name created with OpenDNS.

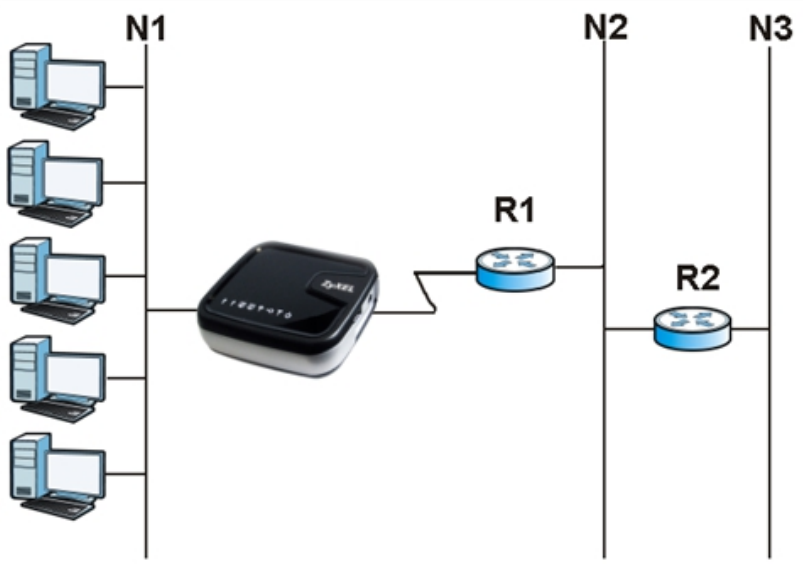
16 Static Route

16.1 Overview

This chapter shows you how to configure static routes for your MWR222.

Each remote node specifies only the network to which the gateway is directly connected, and the MWR222 has no knowledge of the networks beyond. For instance, the MWR222 knows about network N2 in the following figure through remote node Router 1. However, the MWR222 is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the MWR222 about the networks beyond the remote nodes.

Figure 76 Example of Static Routing Topology



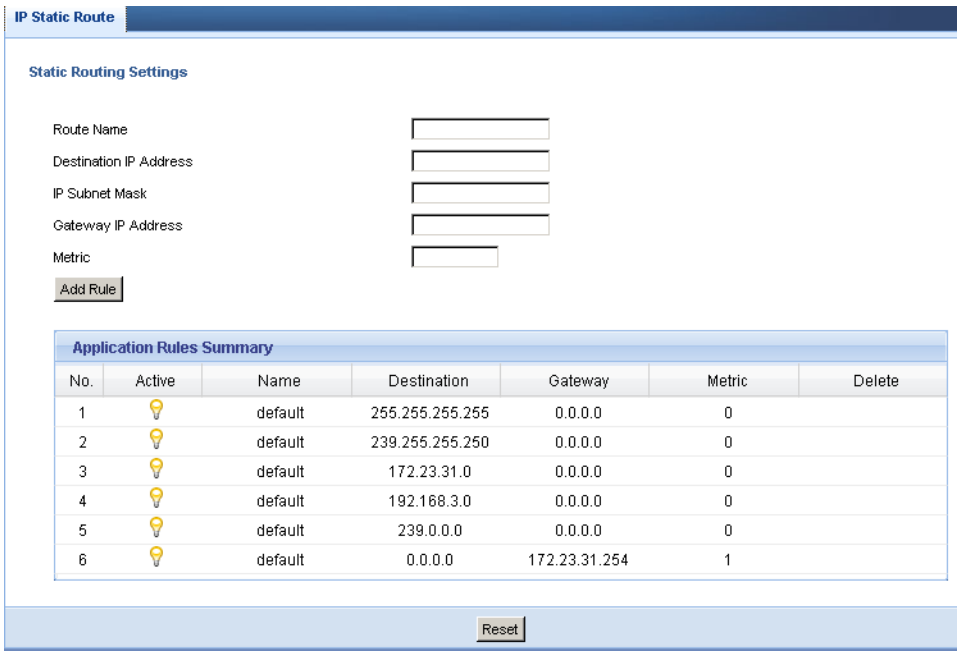
16.2 What You Can Do

Use the **IP Static Route** screen to view, add and delete routes.

16.3 IP Static Route Screen

Click **Network > Static Route** to open the **IP Static Route** screen.

Figure 77 Network > Static Route



The following table describes the labels in this screen.

Table 49 Network > Static Route

LABEL	DESCRIPTION
Static Routing Settings	
Route Name	Enter the name that describes or identifies this route.
Destination IP Address	Enter the IP network address of the final destination.
IP Subnet Netmask	This is the subnet to which the route's final destination belongs.
Gateway IP Address	Enter the IP address of the gateway.
Metric	Assign a number to identify the route.
Add Rule	Click this to add the IP static route.
Application Rules Summary	

No.	This is the number of an individual static route.
Active	The rules are always on and this is indicated by the icon.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	This is the number assigned to the route.
Delete	Click the Delete icon to remove a static route from the MWR222. A window displays asking you to confirm that you want to delete the route.

17. Routing Information Protocol

17.1 Overview

Routing Information Protocol (RIP) is an interior or intra-domain routing protocol that uses distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.

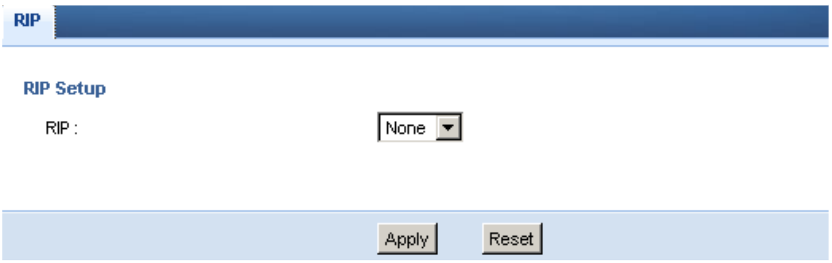
17.2 What You Can Do

Use the **RIP** screen to enable RIPv1 or RIPv2, which are LAN broadcast protocols.

17.3 RIP Screen

Use this screen to enable RIPv1 or RIPv2, which are LAN broadcast protocols. Click **Network > RIP**. The screen appears as shown.

Figure 78 Network > RIP



The following table describes the labels in this screen.

Table 50 Network > RIP

LABEL	DESCRIPTION
RIP	Select the **RIPv1** or **RIPv2** you want the MWR222 to use. Otherwise select **None**.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

Part III
Part III
Security

Firewall

Content Filter

18. Firewall

18.1 Overview

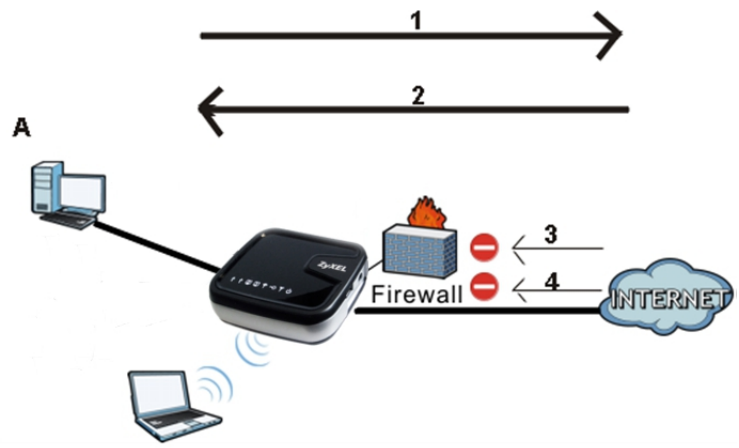
This chapter shows you how to enable and configure the firewall that protects your MWR222 and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- Allows traffic that originates from your LAN computers to go to all of the networks.
- Blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 79 Default Firewall Action



18.2 What You Can Do

- Use the **General** screen to enable or disable the MWR222's firewall.

- Use the **Services** screen screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

18.3 What You Need To Know

The MWR222's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The MWR222's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The MWR222 can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The MWR222 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The MWR222 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

18.4 General Firewall Screen

Use this screen to enable or disable the MWR222's firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

Figure 80 Security > Firewall > General

The following table describes the labels in this screen.

Table 51 Security > Firewall > General

LABEL	DESCRIPTION
Enable DoS	Select this check box to activate the firewall. The MWR222 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

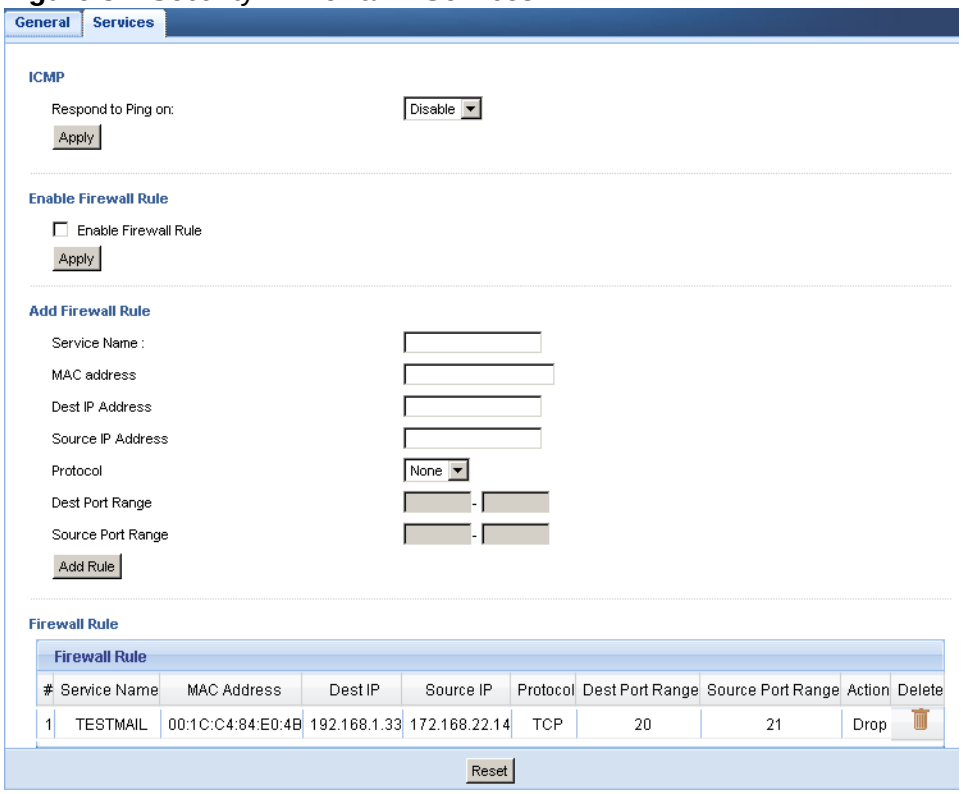
18.5 Services Screen

If an outside user attempts to probe an unsupported port on your MWR222, an ICMP response packet is automatically returned. This allows the outside user to know the MWR222 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your MWR222 when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

Figure 81 Security > Firewall > Services



The following table describes the labels in this screen.

Table 52 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The MWR222 will not respond to any incoming Ping requests when **Disable** is selected. Select **WAN** to reply to incoming WAN Ping requests.
Apply	Click **Apply** to save the settings.

Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below)
Apply	Click **Apply** to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The MWR222 applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The MWR222 applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP**, **ICMP** or **None**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click **Add** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.

MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP**, **ICMP** or **None**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**Drop** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click this to remove the firewall rule.
Reset	Click **Reset** to start configuring this screen again.

See Appendix E for commonly used services and port numbers.

19. Content Filter

19.1 Overview

This chapter provides a brief overview of content filtering using the embedded web GUI.

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

19.2 What You Can Do

Use the **Content Filter** screen to restrict web features, add keywords for blocking and designate a trusted computer.

19.3 What You Need To Know

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages.

19.3.1 Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

Restrict Web Features

The MWR222 can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

Keyword Blocking URL Checking

The MWR222 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL http://us.zyxel.com/Corporate/Pressroom/, the domain name is http://us.zyxel.com/.

The file path is the characters that come after the first slash in the URL. For example, with the URL http://us.zyxel.com/Corporate/Pressroom/, the file path is Corporate/Pressroom.

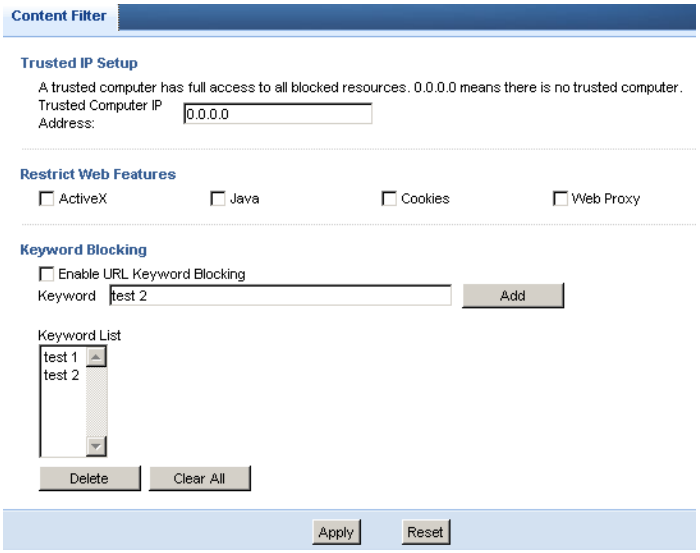
Since the MWR222 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL http://us.zyxel.com/Corporate/Pressroom/, the MWR222 would find "tw" in the domain name (www.us.zyxel.com). It would also find "news" in the file path (Corporate/Pressroom) but it would not find "com/Corporate".

19.4 Content Filter Screen

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer.

Click **Security** > **Content Filter** to open the **Content Filter** screen.

Figure 82 Security > Content Filter > Content Filter



The following table describes the labels in this screen.

Table 53 Security > Content Filter > Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The MWR222 can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.

Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

Part IV
Part IV
Management

Bandwidth Management

Remote Management

Universal Plug-and-Play (UPnP)

20. Bandwidth Management

20.1 Overview

This chapter contains information about configuring bandwidth management and editing rules.

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application.

In the figure below, uplink traffic goes from the LAN device (**A**) to the WAN device (**B**). Bandwidth management is applied before sending the packets out to the WAN. Downlink traffic comes back from the WAN device (**B**) to the LAN device (**A**). Bandwidth management is applied before sending the traffic out to LAN.

Figure 83 Bandwidth Management Example

You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to individual applications (like VoIP, Web, FTP, and E-mail for example).

20.2 What You Can Do

- Use the **General** screen to enable bandwidth management and assign bandwidth values.

- Use the **Advanced** screen to configure bandwidth managements rule for the pre-defined services and applications.
- Use the **Monitor** screen to view the amount of network bandwidth that applications running in the network are using.

20.3 What You Need To Know

The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.

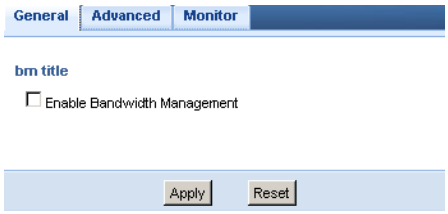
The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.

20.4 General Screen

Use this screen to have the MWR222 apply bandwidth management.

Click **Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

Figure 84 Management > Bandwidth Management > General



The following table describes the labels in this screen.

Table 54 Management > Bandwidth Management > General

LABEL	DESCRIPTION
Enable Bandwidth Management	This field allows you to have MWR222 apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

20.5 Advanced Screen

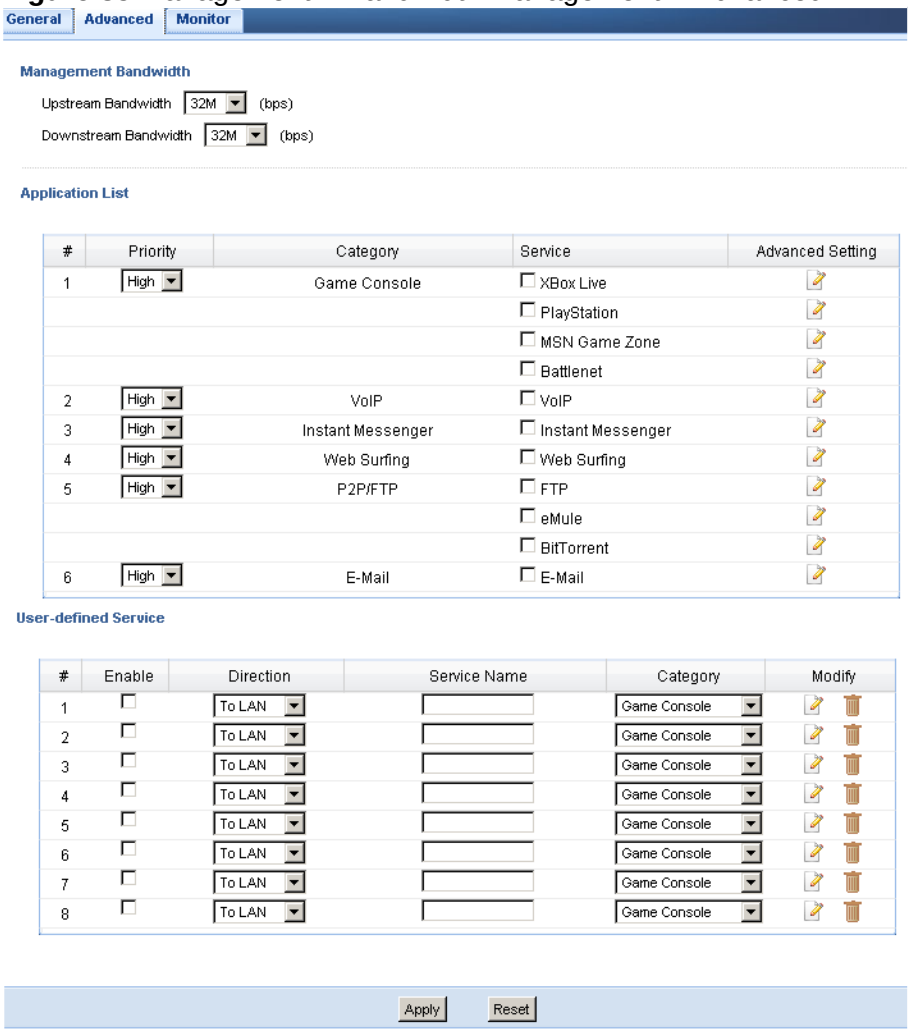
Use this screen to configure bandwidth management rules for the pre-defined services or applications.

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of MWR222. Additionally, you can define the source and destination IP addresses and port for a service or application.

Note: The two tables shown in this screen can be configured and applied at the same time.

Click **Management** > **Bandwidth Management** > **Advanced** to open the bandwidth management **Advanced** screen.

Figure 85 Management > Bandwidth Management > Advanced



The following table describes the labels in this screen.

Table 55 Management > Bandwidth Management > Advanced

LABEL	DESCRIPTION
Management Bandwidth	
Upstream Bandwidth	Select the total amount of bandwidth (from 64 Kilobits to 32 Megabits) that you want to dedicate to uplink traffic. This is traffic from LAN/WLAN to WAN.
Downstream Bandwidth	Select the total amount of bandwidth (from 64 Kilobits to 32 Megabits) that you want to dedicate to uplink traffic. This is traffic from WAN to LAN/WLAN.

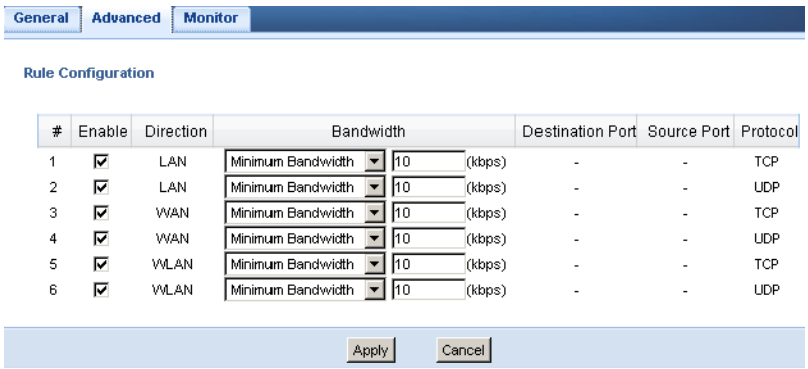
Application List	Use this table to allocate specific amounts of bandwidth based on a pre-defined service.
#	This is the number of an individual bandwidth management rule.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**. • **High** - Select this for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay). • **Mid** - Select this for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. • **Low** - Select this for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Category	This is the category where a service belongs.
Service	This is the name of the service. Select the check box to have the MWR222 apply this bandwidth management rule.
Advanced Setting	Click the **Edit** icon to open the **Rule Configuration** screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications or services you specify.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the MWR222 apply this bandwidth management rule.
Direction	Select **LAN** to apply bandwidth management to traffic from WAN to LAN. Select **WAN** to apply bandwidth management to traffic from LAN/WLAN to WAN. Select **WLAN** to apply bandwidth management to traffic from WAN to WLAN.
Service Name	Enter a descriptive name for the bandwidth management rule.
Category	This is the category where a service belongs.

Modify	Click the **Edit** icon to open the **Rule Configuration** screen. Modify an existing rule or create a new rule in the **Rule Configuration** screen. See Rule Configuration: User Defined Service Rule Co for more information. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

20.5.1 Rule Configuration: Application Rule Configuration

If you want to edit a bandwidth management rule for a pre-defined service or application, click the **Edit** icon in the **Application List** table of the **Advanced** screen. The following screen displays.

Figure 86 Bandwidth Management Rule Configuration: Application List


General
Advanced
Monitor
Rule Configuration
Enable Direction Bandwidth Destination Port Source Port Protocol
1 LAN Minimum Bandwidth 10 (kbps) - - TCP
2 LAN Minimum Bandwidth 10 (kbps) - - UDP
3 WAN Minimum Bandwidth 10 (kbps) - - TCP
4 WAN Minimum Bandwidth 10 (kbps) - - UDP
5 WLAN Minimum Bandwidth 10 (kbps) - - TCP
6 WLAN Minimum Bandwidth 10 (kbps) - - UDP
Apply
Cancel

The following table describes the labels in this screen.

Table 56 Bandwidth Management Rule Configuration: Application List

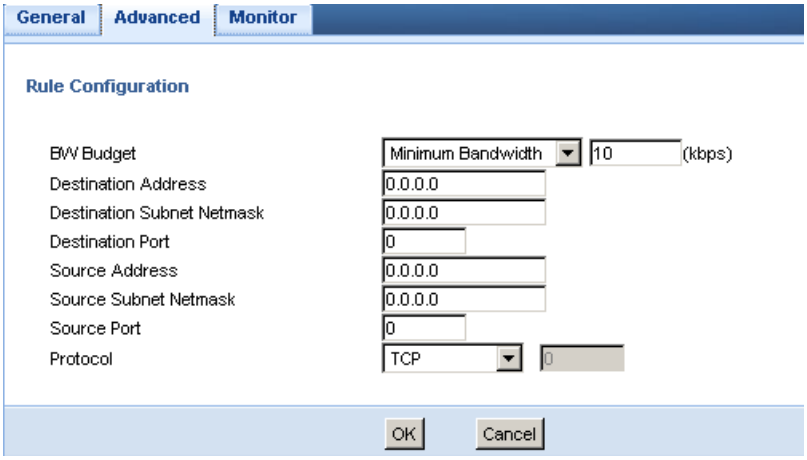
LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the MWR222 and be managed by bandwidth management.

Bandwidth	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic. See Appendix E for some common services and port numbers.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic. See Appendix E for some common services and port numbers.
Protocol	This is the protocol (**TCP**, **UDP** or user-defined) used for the service.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

20.5.2 Rule Configuration: User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for other applications or services, click the **Edit** icon in the **User-defined Service** table of the **Advanced** screen. The following screen displays.

Figure 87 Bandwidth Management Rule Configuration: User-defined Service



The following table describes the labels in this screen

Table 57 Bandwidth Management Rule Configuration: User-defined Service

LABEL	DESCRIPTION
BW Budget	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address	Enter the IP address of the destination computer. The MWR222 applies bandwidth management to the service or application that is entering this computer.
Destination Subnet Netmask	Enter the subnet netmask of the destination of the traffic for which the bandwidth management rule applies.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Address	Enter the IP address of the computer that initializes traffic for the application or service. The MWR222 applies bandwidth management to traffic initiating from this computer.
Source Subnet Netmask	Enter the subnet netmask of the computer initiating the traffic for which the bandwidth management rule applies.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic.
Protocol	Select the protocol (**TCP**, **UDP**, **User defined**) for which the bandwidth management rule applies. If you select **User-defined**, enter the protocol for which the bandwidth management rule applies. For example, ICMP for ping traffic.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

See Appendix E for commonly used services and port numbers.

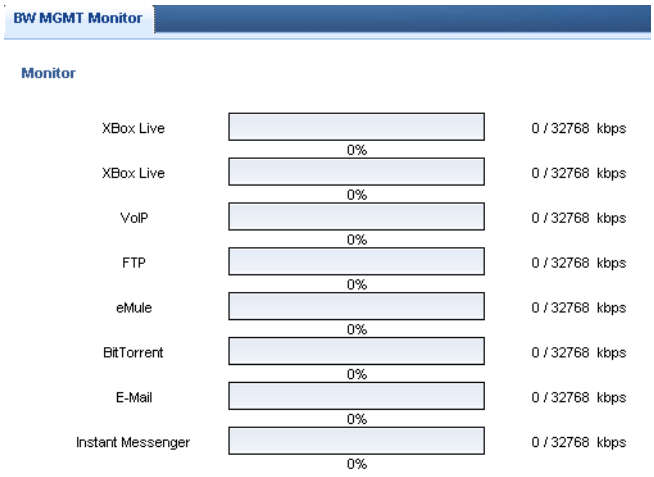
20.6 Monitor Screen

Use this screen to view the amount of network bandwidth that applications running in the network are using.

The bandwidth is measured in kilobits per second (kbps).

The monitor shows what kinds of applications are running in the network, the maximum kbps that each application can use, as well as the percentage of bandwidth it is using.

Figure 88 Management > Bandwidth Management > Monitor



20.6.1 Predefined Bandwidth Management Services

The following is a description of some services that you can select and to which you can apply media bandwidth management in the **Management** > **Bandwidth Management** > **Advanced** screen.

Table 58 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-

	mail:
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files. BitTorrent requires you to search for a file with a search engine yourself. The client downloads the file in small pieces and shares the pieces with other peers to get the other pieces of the file.
Gaming	Online gaming services let you play multiplayer games on the Internet via broadband technology. As of this writing, your MWR222 supports Xbox, Playstation, Battlenet and MSN Game Zone.

21. Remote Management

21.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your MWR222 from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only
- SNMP v1

Note: The MWR222 is managed using the Web Configurator.

21.2 What You Can Do

Use the **WWW** screen (WWW) to define the interface/s from which the MWR222 can be managed remotely and specify a secure client that can manage the MWR222.

Use the **SNMP** (Simple Network Management Protocol) screen (Section 22.5) to enable SNMP v1 management for the MWR222.

21.3 What You Need to Know

Remote management over LAN or WAN will not work when:

1. The IP address in the **Secured Client IP Address** field (WWW) does not match the client IP address. If it does not match, the MWR222 will disconnect the session immediately.
2. There is already another remote management session. You may only have one remote management session running at one time.
3. There is a firewall rule that blocks it.
4. Some mobile WAN ISP blocks remote management. (for example, Verizon allows it but AT&T and Sprint does not.)

21.3.1 Remote Management and NAT

When NAT is enabled:

- Use the MWR222's WAN IP address when configuring from the WAN.
- Use the MWR222's LAN IP address when configuring from the LAN.

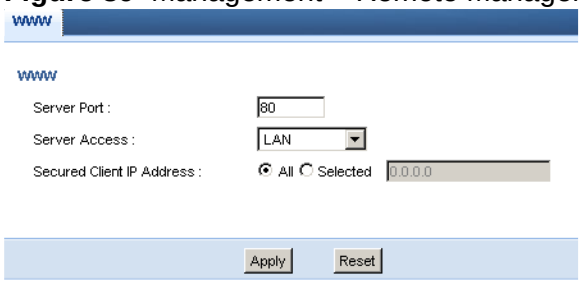
21.3.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The MWR222 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

21.4 WWW Screen

To change your MWR222's remote management settings, click **Management > Remote Management > WWW**.

Figure 89 Management > Remote Management > WWW



The following table describes the labels in this screen

Table 59 Management > Remote Management > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the MWR222 using this service.
Secured Client IP Address	Select **All** to allow all computes to access the MWR222. Otherwise, check **Selected** and specify the IP address of the computer that can access the MWR222.

Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

21.5 SNMP Screen

To configure your MWR222's SNMP settings, click **Management > Remote Management > SNMP**.

Figure 90 Management > Remote Management > SNMP

The following table describes the labels in this screen.

Table 60 Management > Remote Management > SNMP

LABEL	DESCRIPTION
Enable SNMP	Select the **Enable SNMP** check box to enable the SNMP functions.
SNMP Version	Select the SNMP Version used by your management utility. Currently MWR222 only supports v1.
Get / Set Community	Enter the Community name used by your SNMP devices and programs. Devices not in the same Community will not be able to communicate with each other.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

22. Universal Plug-and-Play (UPnP)

22.1 Overview

This chapter introduces the UPnP feature in the web configurator.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

22.2 What You Can Do

Use the UPnP screen to enable UPnP on your MWR222.

22.3 What You Need to Know

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

22.3.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

22.3.2 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the MWR222 allows multicast messages on the LAN only.

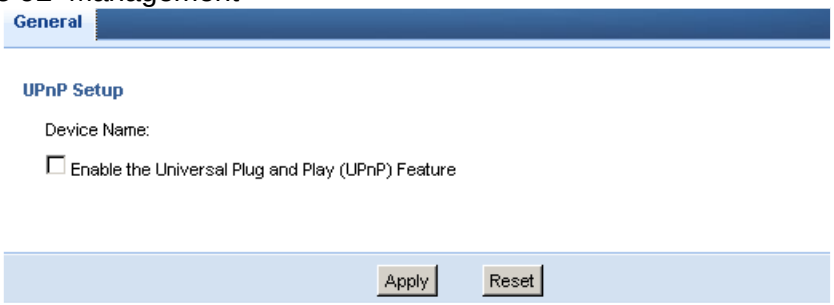
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

22.4 UPnP Screen

Use this screen to enable UPnP on your MWR222.

Click **Management > UPnP** to display the screen shown next.

Figure 91 Management > UPnP



The following table describes the fields in this screen.

Table 61 Management > UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the MWR222's IP address (although you must still enter the password to access the web configurator).

Apply	Click **Apply** to save the setting to the MWR222.
Cancel	Click **Cancel** to return to the previously saved settings.

22.5 Technical Reference

The sections show examples of using UPnP.

22.5.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the MWR222.

Make sure the computer is connected to a LAN port of the MWR222. Turn on your computer and the MWR222.

22.5.1.1 Auto-discover Your UPnP-enabled Network Device

1. Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
2. Right-click the icon and select **Properties**.

Figure 92 Network Connections

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 93 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 94 Internet Connection Properties: Advanced Settings

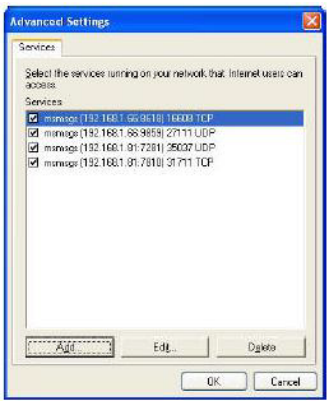


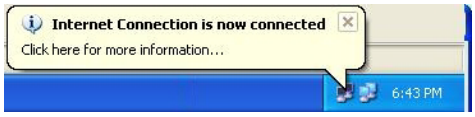
Figure 95 Internet Connection Properties: Advanced Settings:

Add

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 96 System Tray Icon



6 Double-click on the icon to display your current Internet connection status.

Figure 97 Internet Connection Status

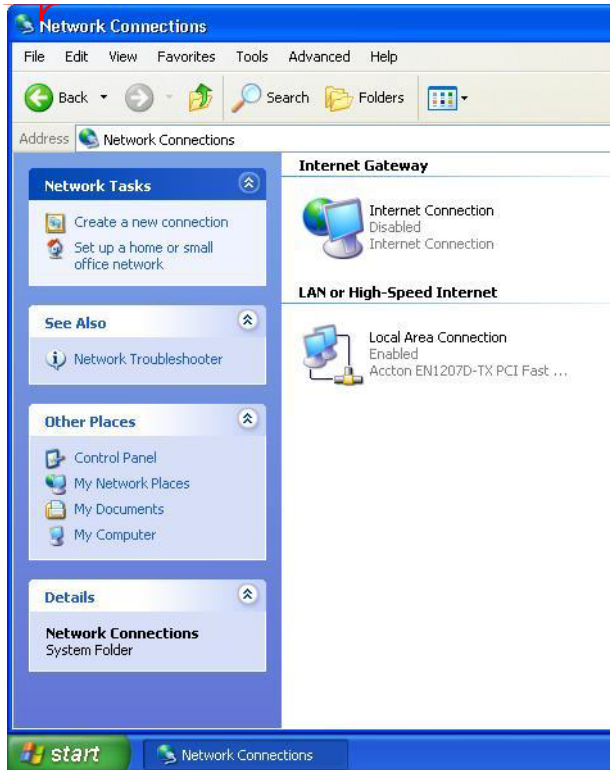
22.5.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the MWR222 without finding out the IP address of the MWR222 first. This comes helpful if you do not know the IP address of the MWR222.

Follow the steps below to access the web configurator.

1. Click **Start** and then **Control Panel**.
2. Double-click **Network Connections**.
3. Select **My Network Places** under **Other Places**.

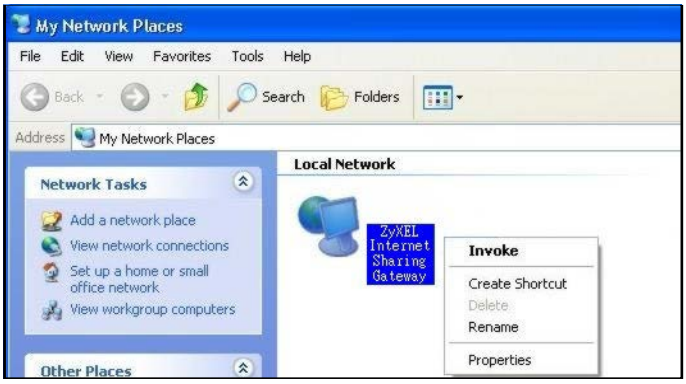
Figure 98 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your MWR222 and select **Invoke**. The web configurator login screen displays.

Figure 99 Network Connections: My Network Places



6 Right-click on the icon for your MWR222 and select **Properties**. A properties window displays with basic information about the MWR222.

Figure 100 Network Connections: My Network Places: Properties: Example

Part V
Maintenance and Troubleshooting

Maintenance

Password

Time

Firmware Upgrade

Backup/Restore/Reset

Restart

Sys OP Mode

Alert

Troubleshooting

23. Maintenance

23.1 Overview

This chapter provides information on the **Maintenance > General** screen.

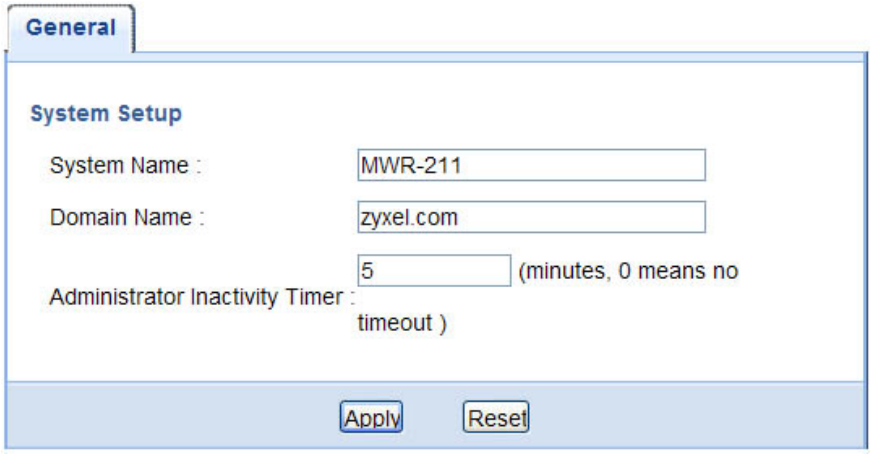
23.2 What You Can Do

- Use the **General** screen to enter a name to identify the MWR222 in the network and set the password.
- Use the **Time Setting** screen to change your MWR222's time and date.

23.3 General Screen

Use this screen to enter a name to identify the MWR222 in the network and set the password. Click **Maintenance** > **General**. The following screen displays.

Figure 101 Maintenance > General



The following table describes the labels in this screen.

Table 62 Maintenance > General

LABEL	DESCRIPTION
System Setup	
System Name	System Name is a unique name to identify the MWR222 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the MWR222.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

24. Password

24.1 Overview

This chapter contains information about configuring general log settings and viewing the MWR222's logs. Refer to the appendices for example log message explanations.

The Web Configurator allows you to look at all of the MWR222's logs in one location.

24.2 What You Can Do

Use the **View Log** screen to see the logs for the categories such as system maintenance, system errors, access control, allowed or blocked web sites, blocked web features, and so on.

24.3 What You Need to Know

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

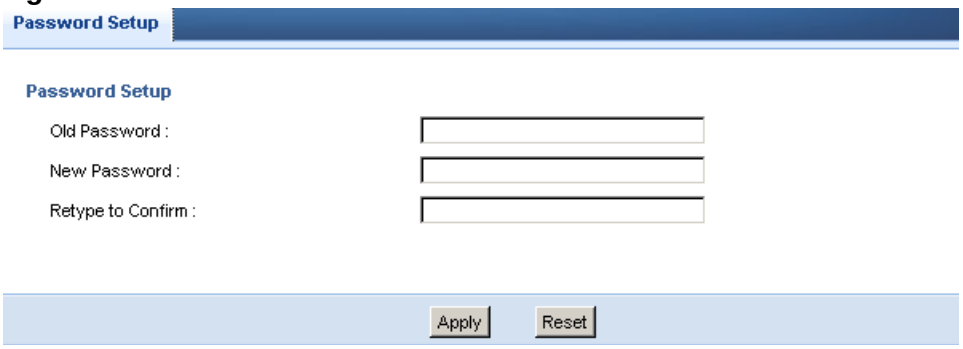
24.4 Password Screen

Use the **View Log** screen to see the logged messages for the MWR222. Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Maintenance** > **Password**.

Figure 102 Maintenance > Password



The following table describes the labels in this screen.

Table 63 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your MWR222's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

25. Time

25.1 Overview

This chapter provides information on the **Time Setting** screens. See Section 3.2.3 for more information on how to set up the MWR222's date and time.

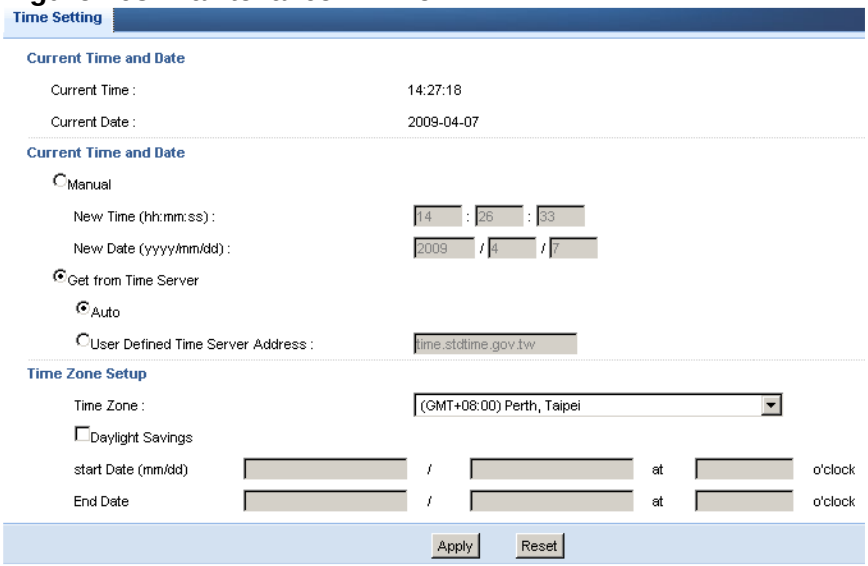
25.2 What You Can Do

Use the Time Setting screen to change your MWR222's time and date.

25.3 Time Setting Screen

Use this screen to configure the MWR222's time based on your local time zone. To change your MWR222's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown.

Figure 103 Maintenance > Time



The following table describes the labels in this screen.

Table 64 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your MWR222. Each time you reload this page, the MWR222 synchronizes the time with the time server.
Current Date	This field displays the date of your MWR222. Each time you reload this page, the MWR222 synchronizes the date with the time server.
Current Time and Date	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the MWR222 get the time and date from the time server you specified below.
Auto	Select **Auto** to have the MWR222 automatically search for an available time server and synchronize the date and time with the time server after you click **Apply**.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.

Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the MWR222.
Reset	Click **Reset** to begin configuring this screen afresh.

26. Firmware Upgrade

26.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the MWR222.

26.2 What You Can Do

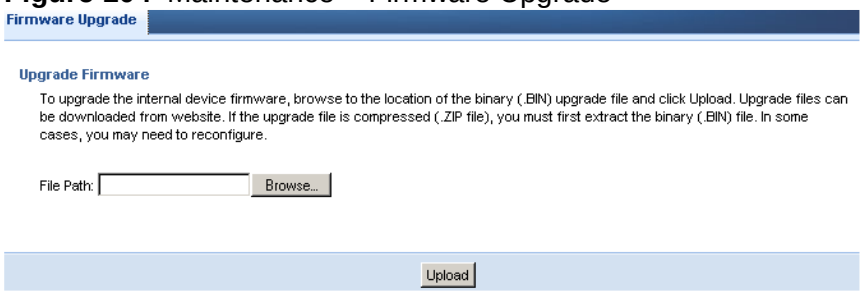
Use the **Firmware** screen to upload firmware to your MWR222.

26.3 Firmware Upload Screen

Find firmware at http://us.zyxel.com/Support/Download-Library.aspx. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your MWR222.

Figure 104 Maintenance > Firmware Upgrade


Firmware Upgrade
Upgrade Firmware
To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.
File Path:
Browse...
Upload

The following table describes the labels in this screen.

Table 65 Maintenance > Firmware Upgrade

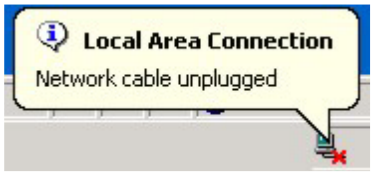
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the MWR222 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the MWR222 again.

The MWR222 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 105 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware** screen.

27. Backup/Restore/ Reset

27.1 Overview

This chapter shows you how to backup, restore and reset your MWR222.

Backup configuration allows you to back up (save) the MWR222's current configuration to a file on your computer. Once your MWR222 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your MWR222.

Reset configuration allows you to restore the configuration to factory default.

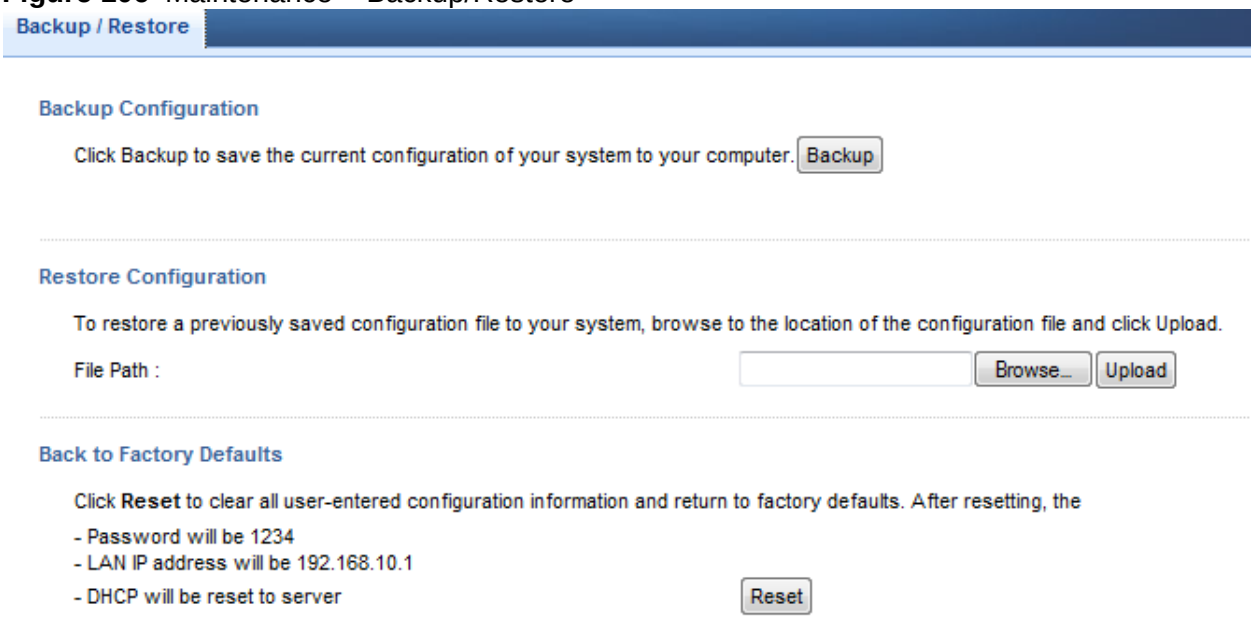
27.2 What You Can Do

Use the **Backup / Restore / Reset** screen to view information related to factory defaults, backup configuration, and restoring configuration.

27.3 Configuration Screen

Click **Maintenance > Backup / Restore / Reset**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 106 Maintenance > Backup/Restore


Backup / Restore
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.10.1
- DHCP will be reset to server
Reset

The following table describes the labels in this screen.

Table 66 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the MWR222's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the MWR222 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the MWR222 again. The MWR222 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.

Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the MWR222 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your MWR222. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default MWR222 IP address (192.168.10.1). See Appendix C for details on how to set up your computer's IP address.

28. Restart

28.1 Overview

This chapter shows you how to restart your MWR222.

28.2 What You Can Do

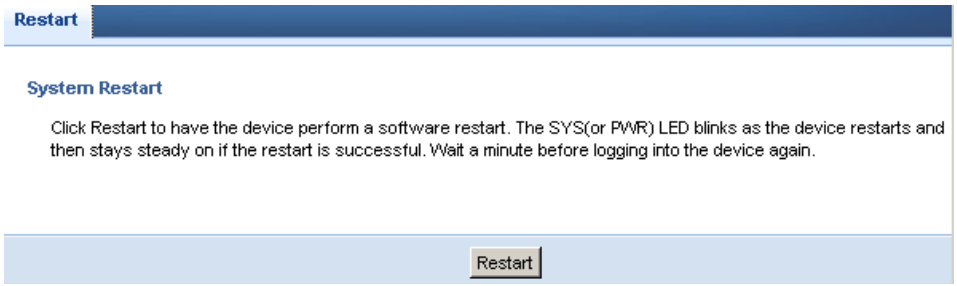
Use the **Restart** screen to boot the MWR222 without turning the power off.

28.3 Restart Screen

System restart allows you to reboot the MWR222 without turning the power off.

Click **Maintenance > Restart** to open the following screen.

Figure 107 Maintenance > Reset/Restart


Restart
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

Click **Restart** to have the MWR222 reboot. This does not affect the MWR222's configuration.

29. Sys OP Mode

29.1 Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure your MWR222 as a router, access point or Wireless ISP (WISP) client. You can choose between **Router Mode**, **Access Point Mode** and **WISP Mode** depending on your network topology and the features you require from your device.

See Section 5.1.2 for more information on which mode to choose.

29.2 What You Can Do

Use the **Sys OP Mode** screen (Sys Op Mode Screen) to select how you want to use your MWR222.

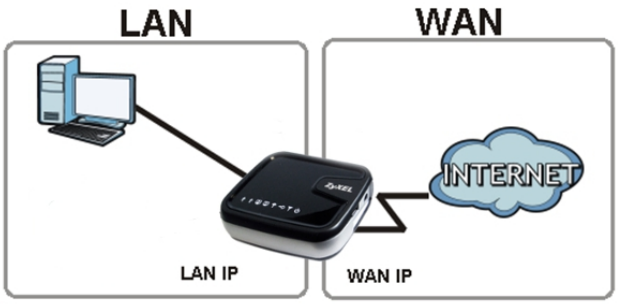
29.3 What You Need to Know

The following describes the device modes available in your MWR222.

Router

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

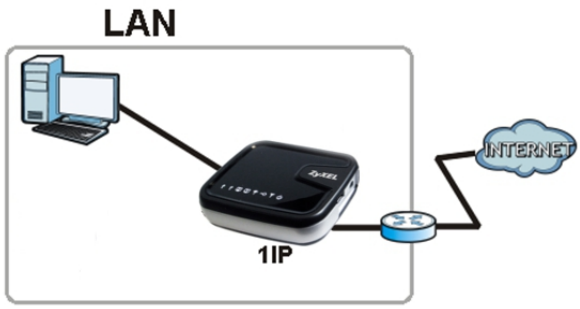
Figure 108 LAN and WAN IP Addresses in Router Mode



Access Point

An access point enabled all Ethernet ports to be bridged together and be in the same subnet. To connect to the Internet, another device, such as a router, is required.

Figure 109 IP Address in Access Point Mode



WISP

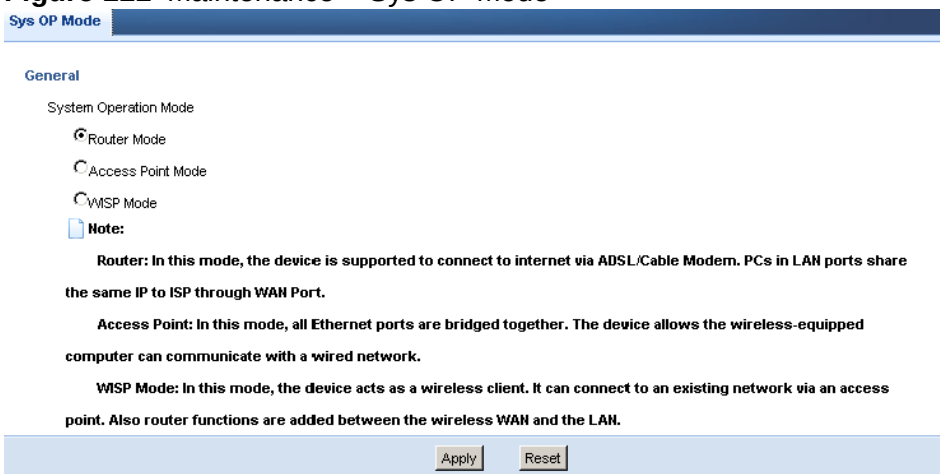
A WISP client connects to an existing access point wirelessly. It acts just like a wireless client in notebooks/computers.

Figure 110 IP Address in Access Point Mode

29.4 Sys Op Mode Screen

Use this screen to select how you want to use your MWR222.

Figure 111 Maintenance > Sys OP Mode


Sys OP Mode
General
System Operation Mode
Router Mode
Access Point Mode
WISP Mode
Note:
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.
Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.
WISP Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.
Apply
Reset

The following table describes the labels in the **General** screen.

Table 67 Maintenance > Sys OP Mode

LABEL	DESCRIPTION
System Operation Mode	
Router	Select **Router Mode** if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management. You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.
Access Point	Select **Access Point Mode** if your device bridges traffic between clients on the same network. • In Access Point mode all Ethernet ports have the same IP address. • All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port. • The DHCP server on your device is disabled. • The IP address of the device on the local network is set to 192.168.10.2.

WISP Mode	Select **WISP Mode** if your device needs a wireless client to connect to an existing access point. • You cannot configure Wireless LAN settings (including WPS) and scheduling in the WISP mode. • The IP address of the device on the local network is the same as the IP address given to the MWR222 while in router mode (default is 192.168.10.1).
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return your settings to the default (**Router**)

Note: If you select the incorrect System Operation Mode you may not be able to connect to the Internet.

30. Alert

30.1 Overview

The **Alert** (SMTP) function enable MWR222 sends mobile data usage alert to the users. When the router has downloaded data reaching 90% of the usage allowance, the quota manager will send a warning alert to the users (if the Email-Alert is enabled) and /or post a log to the system. All the subsequent alerts will indicate the percentage of the current quota usage in the email and/or log as well.

See Section 5.1.2 for more information on which mode to choose.

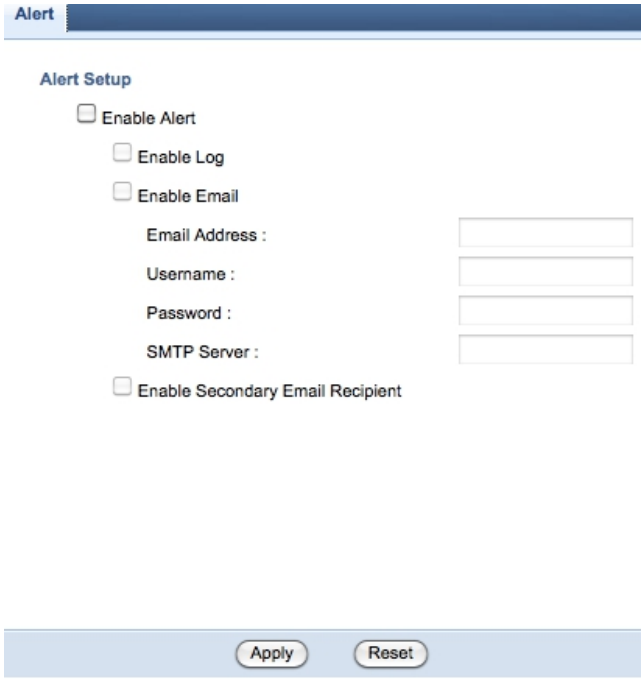
30.2 What You Can Do

Use the **Alert** screen to select how you want your MWR222 to contact you with alerts.

30.3 Alert Screen

Use this screen to select the Alert settings for your MWR222.

Figure 112 Maintenance > Alert



The following table describes the labels in the **Alert** screen.

Table 68 Maintenance > Alert

LABEL	DESCRIPTION
Enable Alert	Select **Enable Alert** to use the alert functions of the MWR222.
Enable Log	Select **Enable Log** to send system log information in the alert.
Enable Email	Select **Enable Email** to allow alert information to be sent by email.
Email Address	Type the Email Address you want the alerts sent to.
Username	Type the Username required by your SMTP Server.
Password	Type the password associated with the Username above.
SMTP Server	Type the address of your SMTP server.

Enable Secondary Email Recipient	Select **Enable Secondary Email Recipient** to set up a second email address to send alerts to.
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return your settings to the default (**Router**)

31 Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Internet Access
- Resetting
- Wireless Router/AP Troubleshooting

31.1 Power, Hardware Connections, and LEDs

The MWR222 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the MWR222.
2. Make sure the power adaptor or cord is connected to the MWR222 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the MWR222.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5.

2 Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor to the MWR222.

5 If the problem continues, contact the vendor.

31.2 MWR222 Access and Login

I don't know the IP address of my MWR222.

1 The default IP address is **192.168.10.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the MWR222 by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the MWR222 (it depends on the network), so enter this IP address in your Internet browser. Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your MWR222's IP address is available in the **Device Information** table.

- If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
- If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.

3 If your MWR222 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your MWR222 to change all settings back to their default. This means your current settings are lost. See Resetting in the **Troubleshooting** for information on resetting your MWR222.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Resetting .

I cannot see or access the **Login** screen in the Web Configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.10.1.
   - If you changed the IP address (Section 13.4), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A.
4. Make sure your computer is in the same subnet as the MWR222. (If you know that there are routers between your computer and the MWR222, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 14.3.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the MWR222. See Appendix B.
5. Reset the device to its factory defaults, and try to access the MWR222 with the default IP address. See Section 28.3.
6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

I can see the **Login** screen, but I cannot log in to the MWR222.

1. Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
2. This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
3. Disconnect and re-connect the power adaptor or cord to the MWR222.
4. If this does not work, you have to reset the device to its factory defaults. See Resetting .

31.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

2. Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
   - Go to Network > Wireless LAN > General > WDS and check if the MWR222 is set to bridge mode. Select **Disable** and try to connect to the Internet again.

4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5. Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
   - Select **Router** if your device routes traffic between a local network and another network such as the Internet.
   - Select **Access Point** if your device bridges traffic between clients on the same network.

6. If the problem continues, contact your ISP.

I cannot access the Internet though mobile WAN

1. Make sure your 3G adapter is activated, account is valid with your Internet service provider

2. Make sure you have configured the mobile WAN port correctly.

3. Disconnect the 3G adapter from the USB port, and follow the directions in the Quick Start Guide again.

5. Make sure you have selected router mode under Sys OP mode configuration page.

I cannot access the Internet anymore. I had access to the Internet (with the MWR222), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5.

2. Reboot the MWR222.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5. If the MWR222 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving the MWR222 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Reboot the MWR222.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

31.4 Resetting MWR222 to Factory Defaults

If you reset the MWR222, you lose all of the changes you have made. The MWR222 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the MWR222,

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than 1 second to restart/reboot the MWR222.

3 Press the **RESET** button for longer than five seconds to set the MWR222 back to its factory-default configurations.

If the MWR222 restarts automatically, wait for the MWR222 to finish restarting, and log in to the Web Configurator. The password is “1234”.

If the MWR222 does not restart automatically, disconnect and reconnect the MWR222’s power. Then, follow the directions above again.

31.5 Wireless Router/AP Troubleshooting

I cannot access the MWR222 or ping any computer from the WLAN (wireless AP or router).

1. Make sure the wireless LAN is enabled on the MWR222
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the MWR222.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the MWR222.
5. Check that both the MWR222 and your wireless station are using the same wireless and wireless security settings.
6. Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the MWR222.
7. Make sure you allow the MWR222 to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User’s Guide for more information.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

I can access the Internet, but I cannot open my network folders.

In the Network > LAN > Advanced screen, make sure **Allow between LAN and WAN** is checked. This is not checked by default to keep the LAN secure.

If you still cannot access a network folder, make sure your account has access rights to the folder you are trying to open.

I can access the Web Configurator after I switched to AP mode.

When you change from router mode to AP mode, your computer must have an IP address in the range between “192.168.10.3” and “192.168.10.254”.

Refer to Appendix C for instructions on how to change your computer’s IP address.

The following tables summarize the MWR222’s hardware and firmware features.

Table 69 Hardware Features

Dimensions (W x D x H)	162 mm x 115 mm x 33 mm
Weight	252 g
Power Specification	Input: 100~240 V AC, 50~60 Hz Output: 5V DC 2A
Ethernet ports	Auto-negotiating: 10 Mbps, 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
LEDs	PWR, Battery, LAN/WAN, WLAN, WPS, USB
Reset Button	The reset button is built into the rear panel. Use this button to restore the MWR222 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Wireless Switch	Turn on or turn off the wireless function of the MWR222 using this switch. There is no need to go into the Web Configurator.
Operation Environment	Temperature: 0º C ~ 40º C / 32ºF ~ 104ºF Humidity: 20% ~ 90%
Storage Environment	Temperature: -30º C ~ 70º C / -22ºF ~ 158ºF Humidity: 20% ~ 95%

Table 70 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.10.1 (router) 192.168.10.2. (AP)
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.10.33 to 192.168.10.64
Wireless Interface	Wireless LAN
Default Wireless SSID	ZyXEL
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (32 from 192.168.10.33 to 192.168.10.64)
Device Management	Use the Web Configurator to easily configure the rich range of features on the MWR222.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the MWR222 wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The MWR222 may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the MWR222. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the MWR222's configuration and put it back on the MWR222 later if you decide you want to revert back to an earlier configuration.

Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the MWR222 for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The MWR222 blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering. You can also subscribe to category-based content filtering that allows your MWR222 to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the MWR222.
Wireless LAN Scheduler	You can schedule the times the Wireless LAN is enabled/disabled.
Time and Date	Get the current time and date from an external server when you turn on your MWR222. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the MWR222 assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.

IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The MWR222 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Logging	Use logs for troubleshooting. You can view logs in the Web Configurator.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The MWR222 supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The MWR222 can communicate with other UPnP enabled devices in a network.

32 Product Specifications

The following tables summarize the MWR222's hardware and firmware features.

Table 71 Hardware Features

Dimensions (W x D x H)	162 mm x 115 mm x 33 mm
Weight	252 g
Power Specification	Input: 100~240 V AC, 50~60 Hz Output: 5V DC 2A
Ethernet ports	Auto-negotiating: 10 Mbps, 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
LEDs	PWR, Battery, LAN/WAN, WLAN, WPS, USB
Reset Button	The reset button is built into the rear panel. Use this button to restore the MWR222 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Wireless Switch	Turn on or turn off the wireless function of the MWR222 using this switch. There is no need to go into the Web Configurator.
Operation Environment	Temperature: 0º C ~ 40º C / 32ºF ~ 104ºF Humidity: 20% ~ 90%
Storage Environment	Temperature: -30º C ~ 70º C / -22ºF ~ 158ºF Humidity: 20% ~ 95%

Table 72 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.10.1 (router) 192.168.10.2. (AP)
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.10.33 to 192.168.10.64
Wireless Interface	Wireless LAN
Default Wireless SSID	ZyXEL
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (32 from 192.168.10.33 to 192.168.10.64)
Device Management	Use the Web Configurator to easily configure the rich range of features on the MWR222.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the MWR222 wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The MWR222 may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the MWR222. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the MWR222's configuration and put it back on the MWR222 later if you decide you want to revert back to an earlier configuration.

Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the MWR222 for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The MWR222 blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering. You can also subscribe to category-based content filtering that allows your MWR222 to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the MWR222.
Wireless LAN Scheduler	You can schedule the times the Wireless LAN is enabled/disabled.
Time and Date	Get the current time and date from an external server when you turn on your MWR222. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the MWR222 assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.

IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The MWR222 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Logging	Use logs for troubleshooting. You can view logs in the Web Configurator.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The MWR222 supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The MWR222 can communicate with other UPnP enabled devices in a network.

Part VI Appendices and Index

Pop-up Windows, JavaScripts and Java Permissions

IP Addresses and Subnetting

Setting up Your Computer's IP Address

Wireless LANs

Common Services

Legal Information

Appendix A

Pop-up Windows, JavaScripts and Java Permissions

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

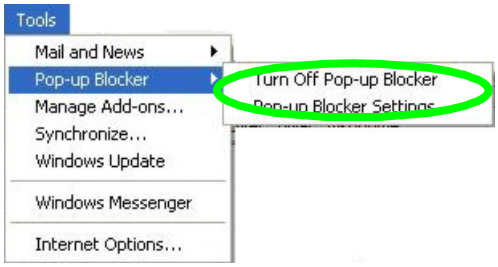
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1. In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

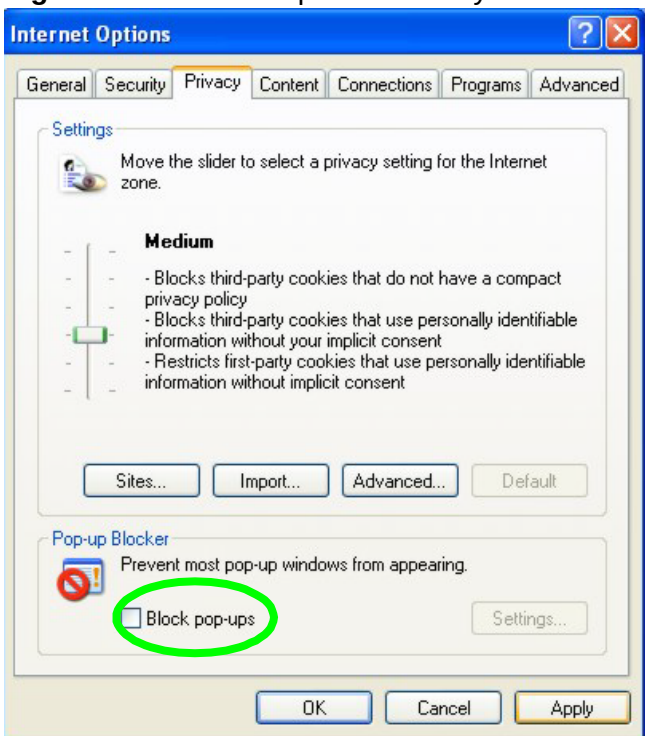
Figure 113 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1. In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
2. Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 114 Internet Options: Privacy



3. Click **Apply** to save this setting.

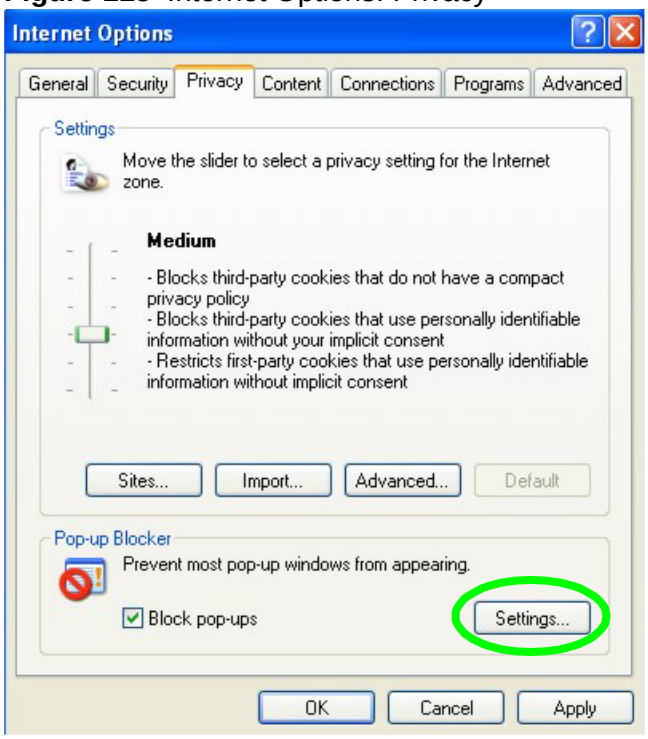
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1. In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 115 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 116 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

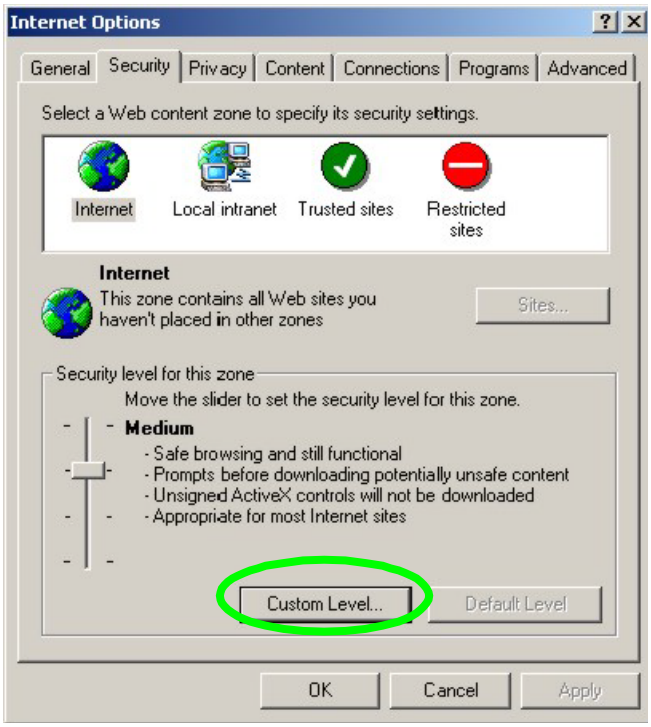
6 Click **Apply** to save this setting.

JavaScripts

If pages of the Web Configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 117 Internet Options: Security



2 Click the **Custom Level...** button.

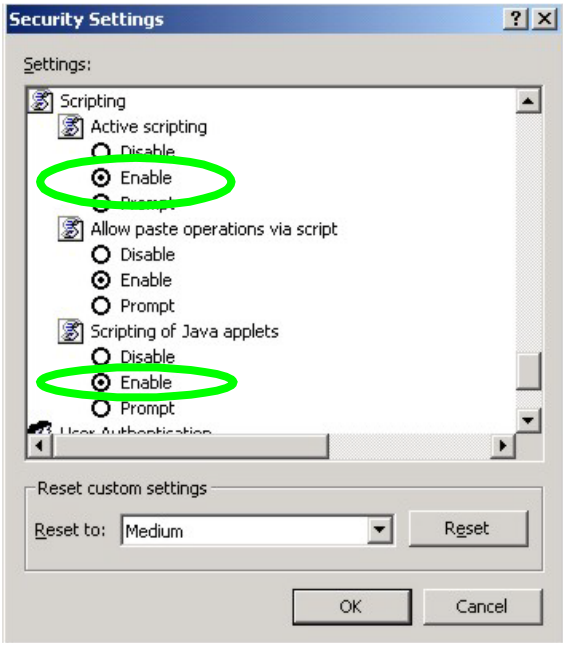
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

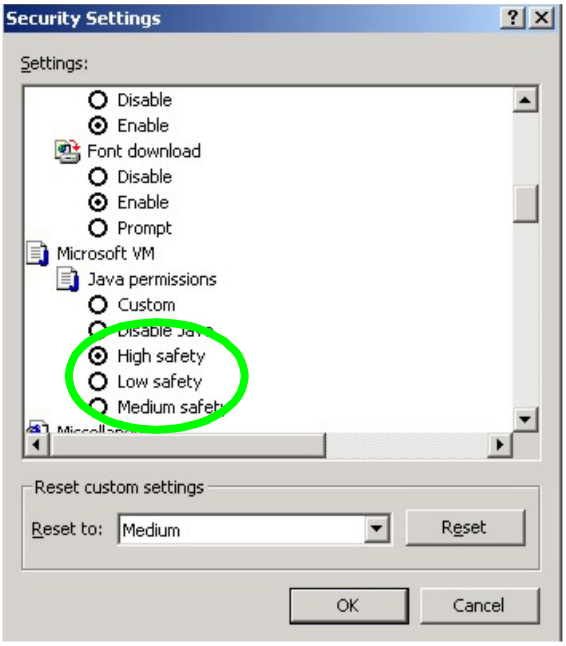
Figure 118 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

Figure 119 Security Settings – Java



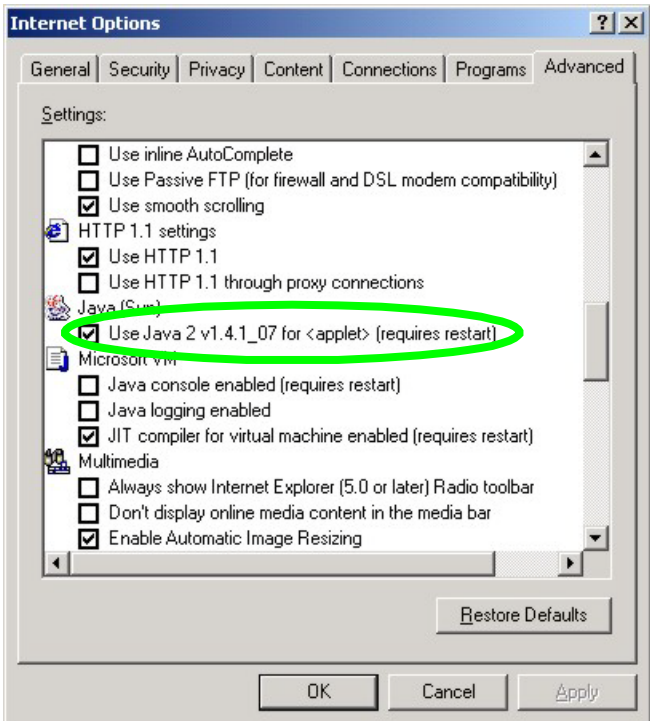
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 120 Java (Sun)



Appendix B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

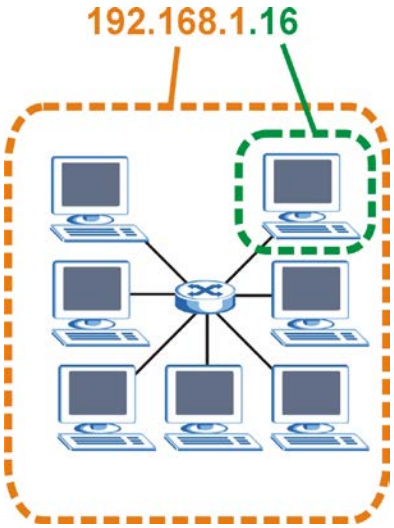
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 121 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 73 Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks

Table 74 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit	11111111	11111111	11111111	00000000	255.255.255.0

mask					
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

.

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 75 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each

octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 76 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

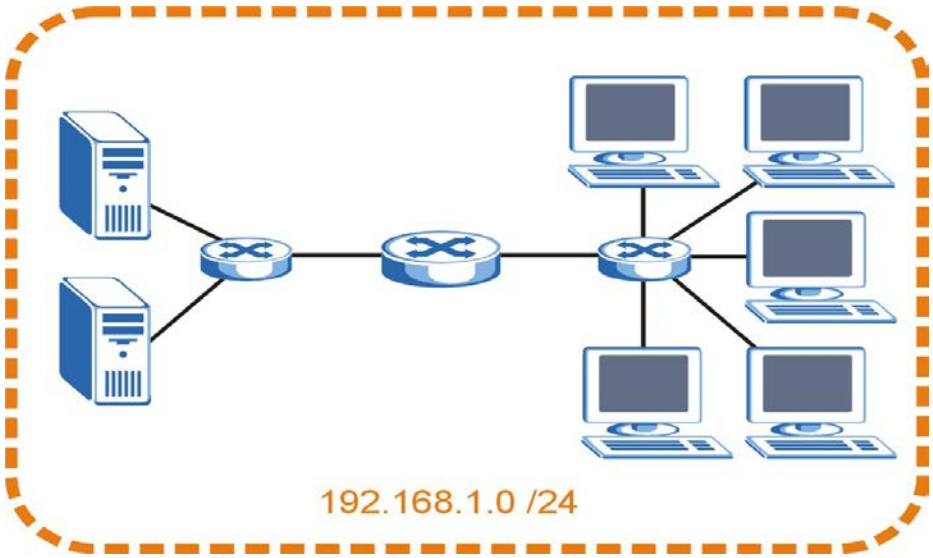
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 122 Subnetting Example: Before Subnetting

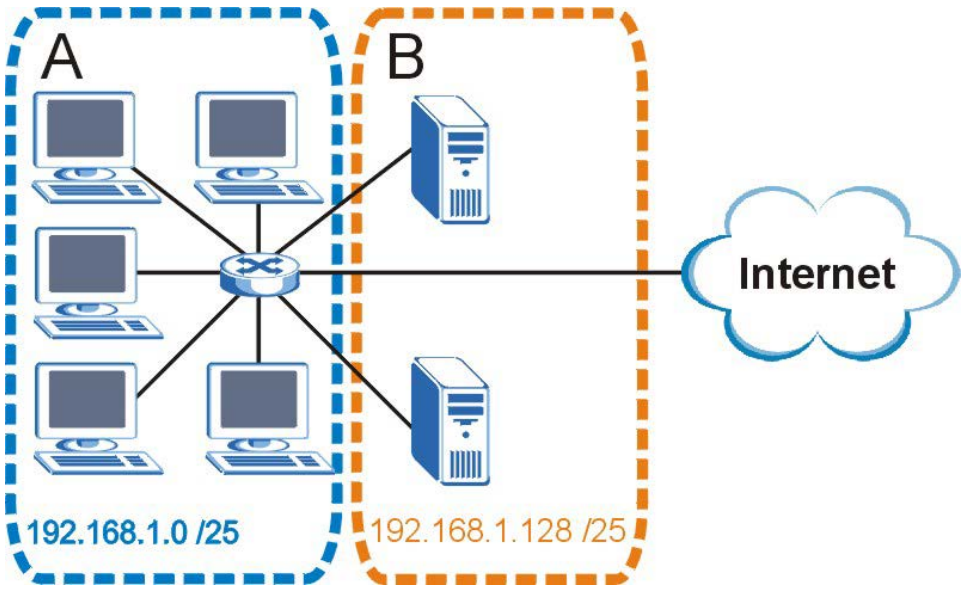


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 123 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 77 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 78 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 79 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 80 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 81 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 82 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126

2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 83 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126

10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the MWR222.

Once you have decided on the network number, pick an IP address for your MWR222 that is easy to remember (for instance, 192.168.10.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your MWR222 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the MWR222 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the

Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

Appendix C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

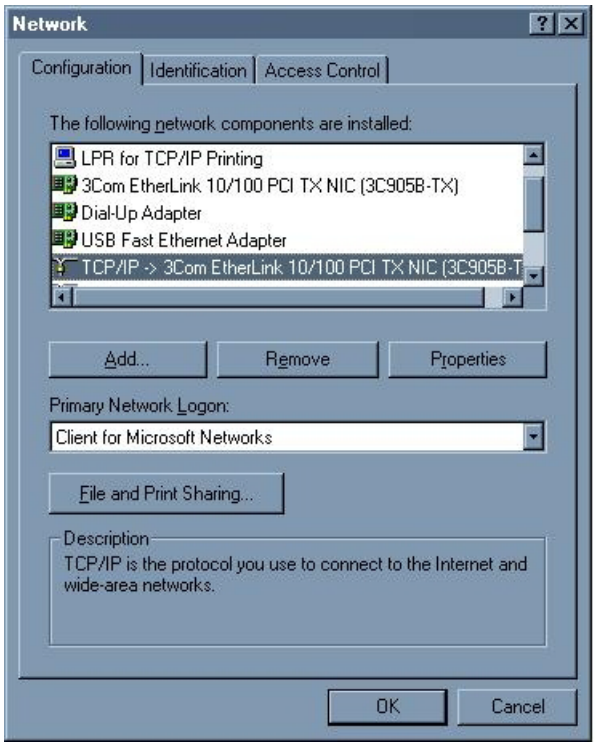
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 124 Windows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

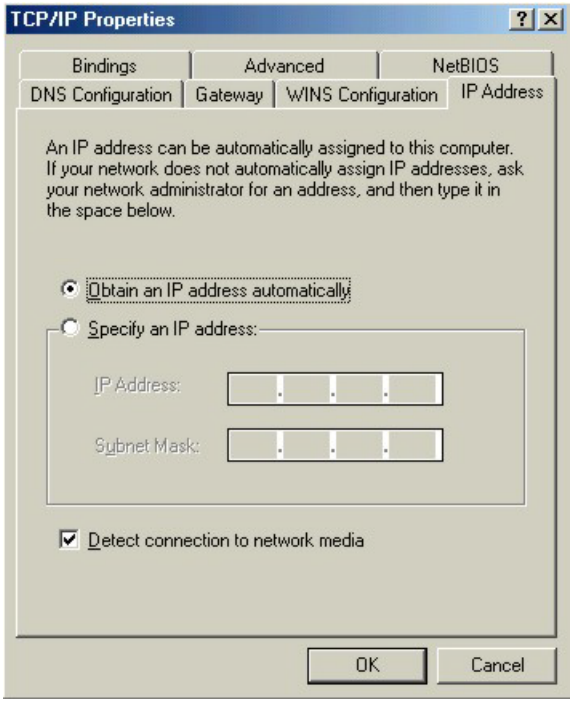
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

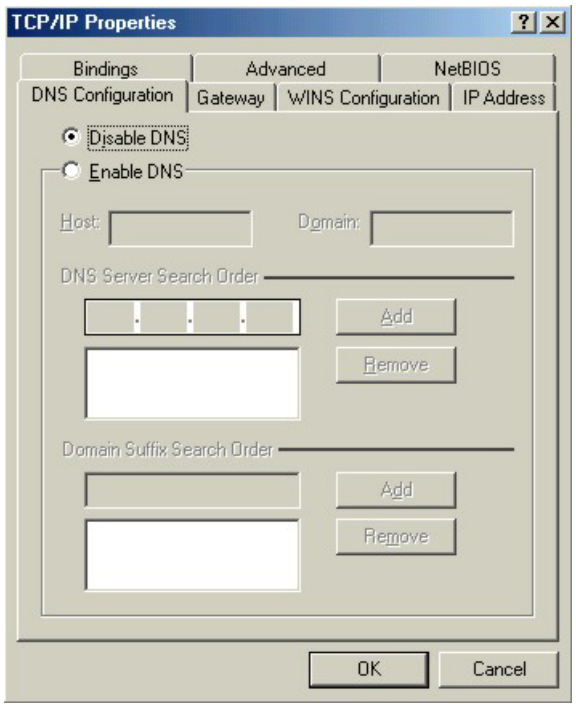
Figure 125 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 126 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP / IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your router and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

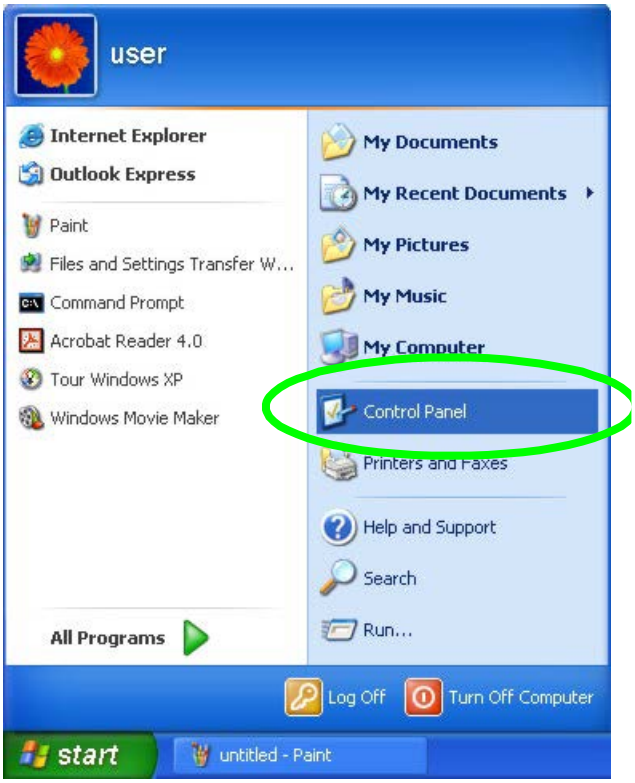
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 127 Windows XP: Start Menu

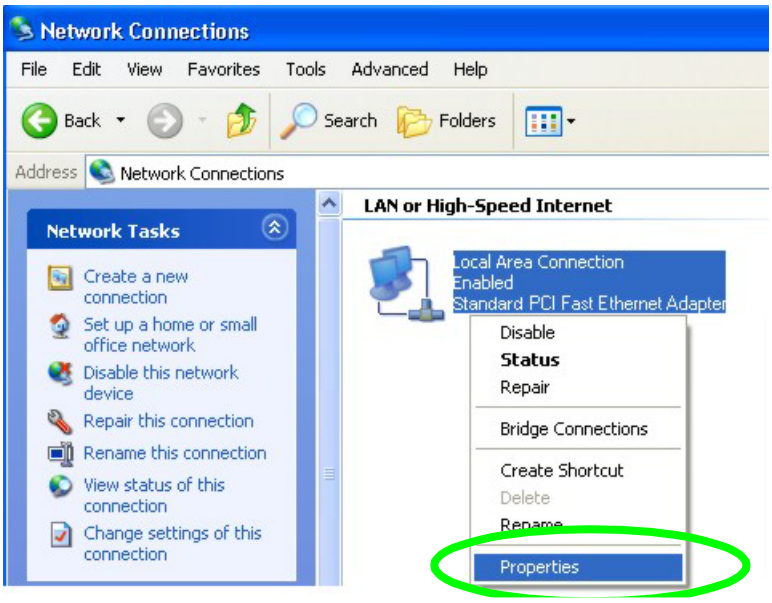


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 128 Windows XP: Control Panel

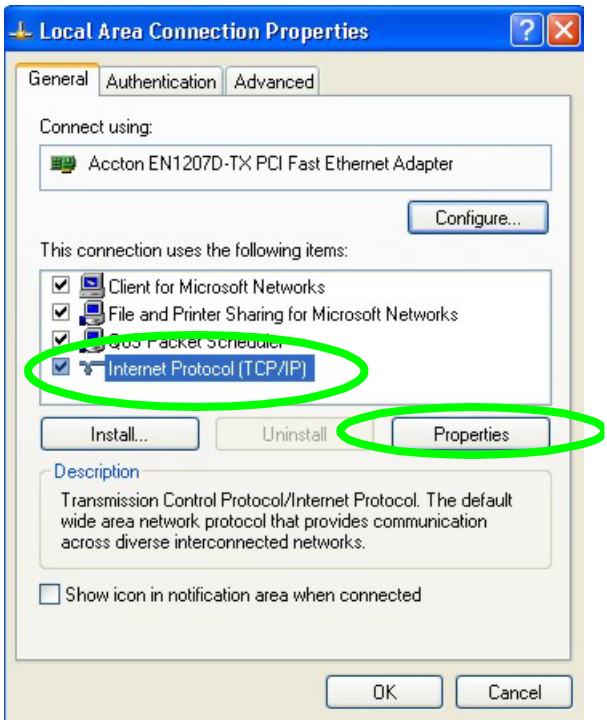
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 129 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 130 Windows XP: Local Area Connection Properties

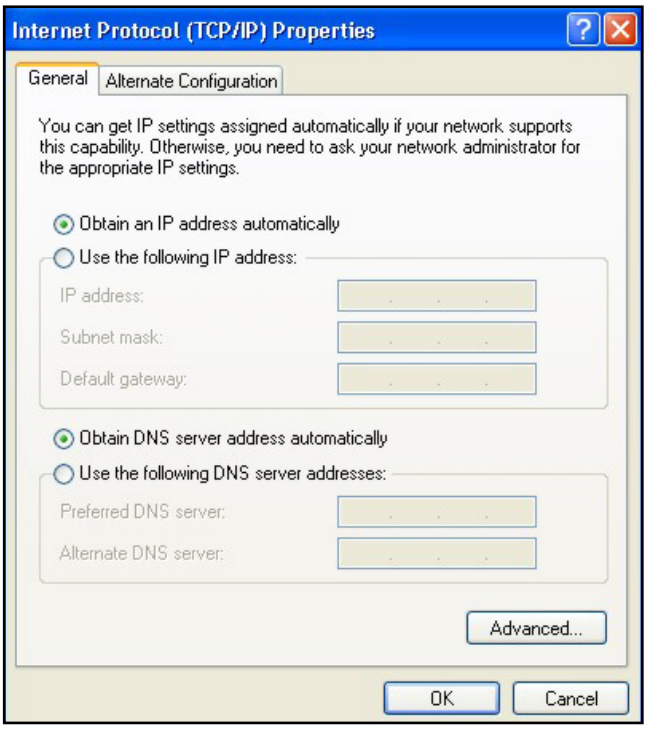

Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

Figure 131 Windows XP: Internet Protocol (TCP/IP) Properties

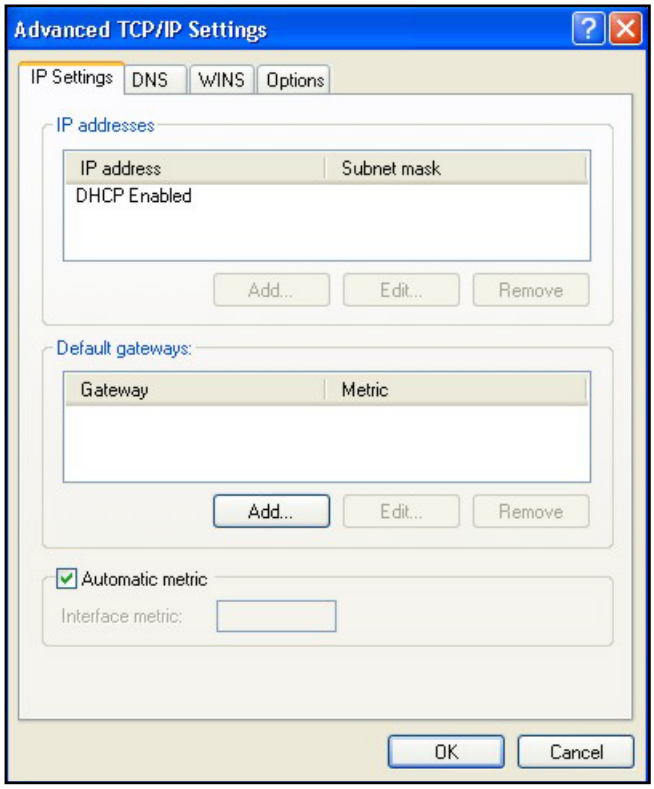

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 132 Windows XP: Advanced TCP/IP Properties

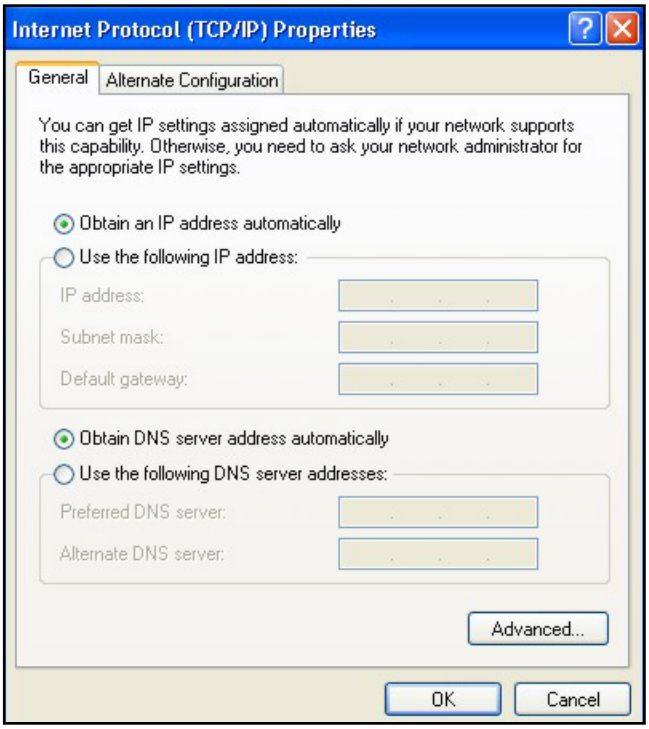


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 133 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your router and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

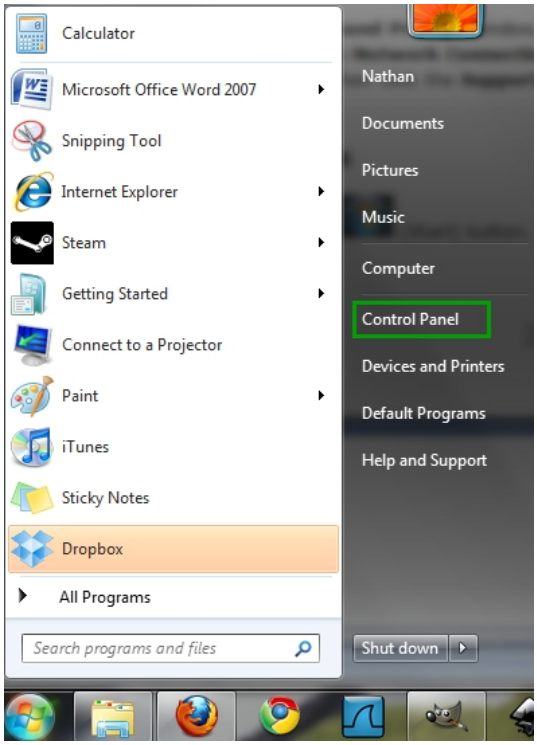
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows 7/Vista

1 Click on the (**Start**) button.

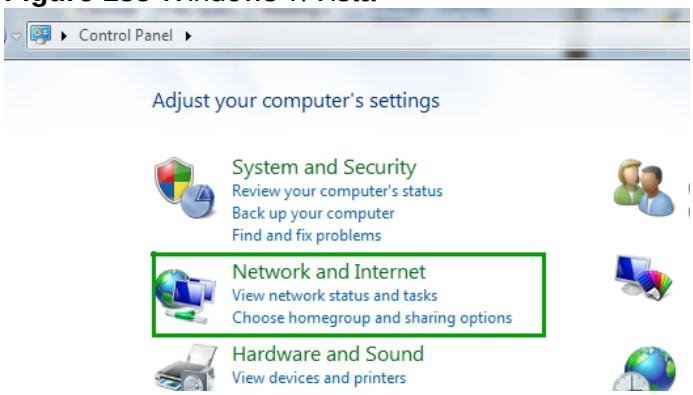
2 Click on **Control Panel.**

Figure 134 Windows 7/Vista



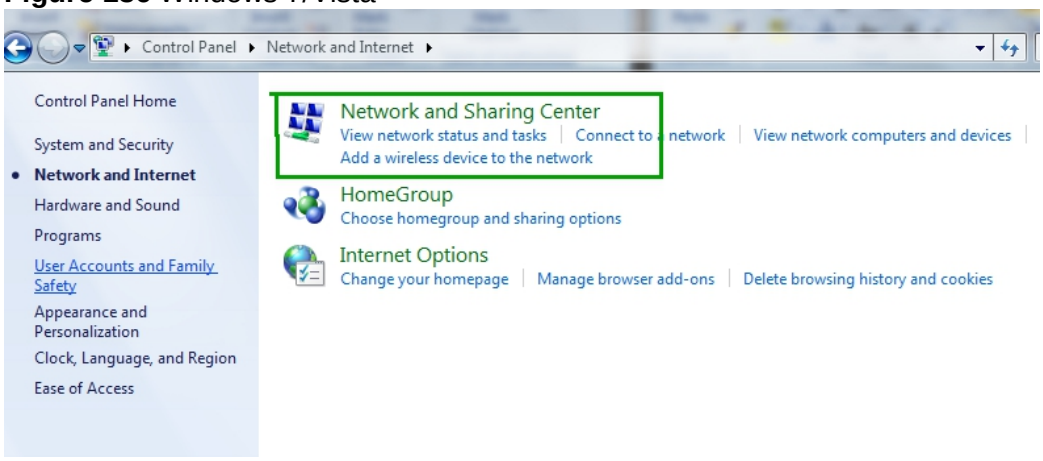
3 Click on **Network and Internet**.

Figure 135 Windows 7/Vista



4 Click on **Network and Sharing Center**

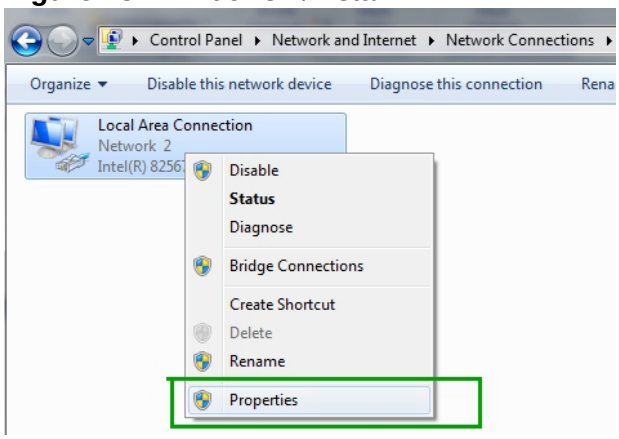
Figure 136 Windows 7/Vista



5 On the left side of the screen click on **Change Adapter Settings** (Windows 7), or **Manage Network Connections** (Vista).

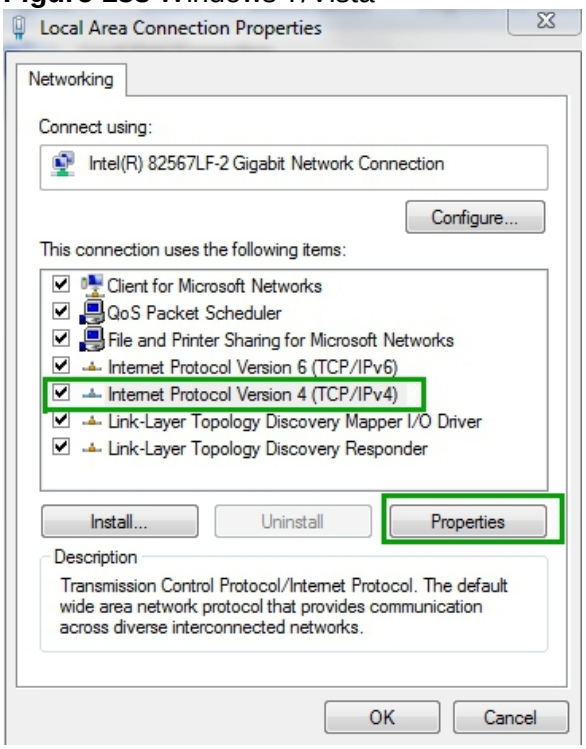
6 Right click on **Local Area Connection** and select **Properties**.

Figure 137 Windows 7/Vista



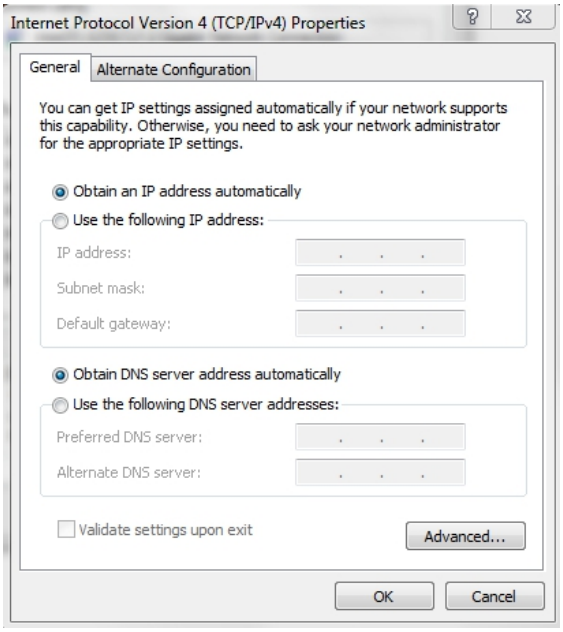
7 Highlight **Internet Protocol Version 4** and click **Properties**.

Figure 138 Windows 7/Vista



8 Select **Use the Following IP Address** and enter your IP address, Subnet Mask, and Default Gateway. Enter your DNS server address (if trying to connect to the internet) and click **OK**.

Figure 139 Windows 7/Vista

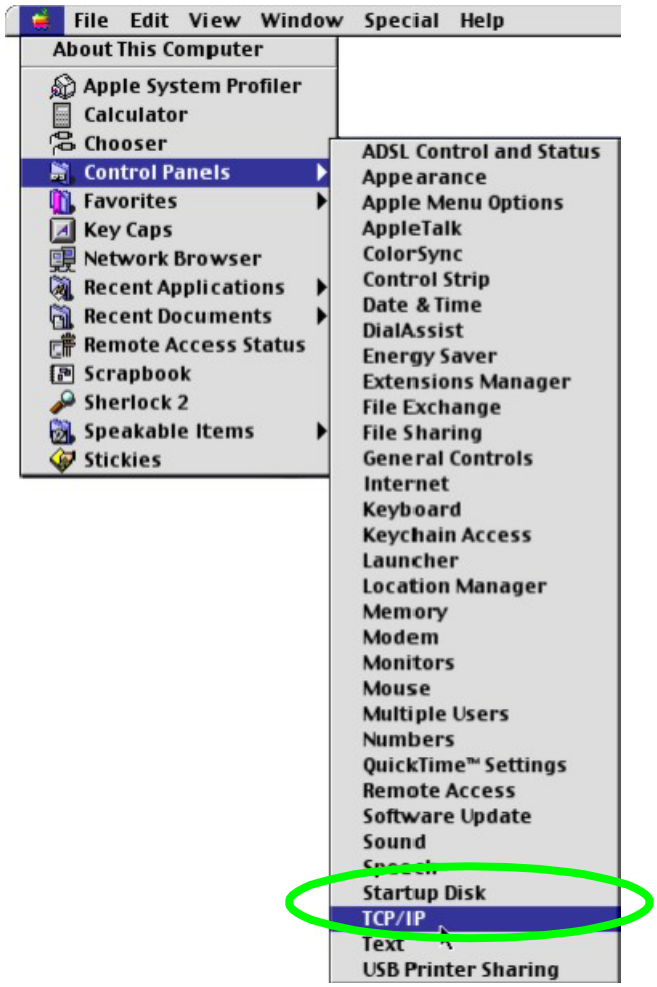

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

9 Click **OK** or **Close** on the Local Area Connection Properties window to apply the settings.

Macintosh OS 8/9

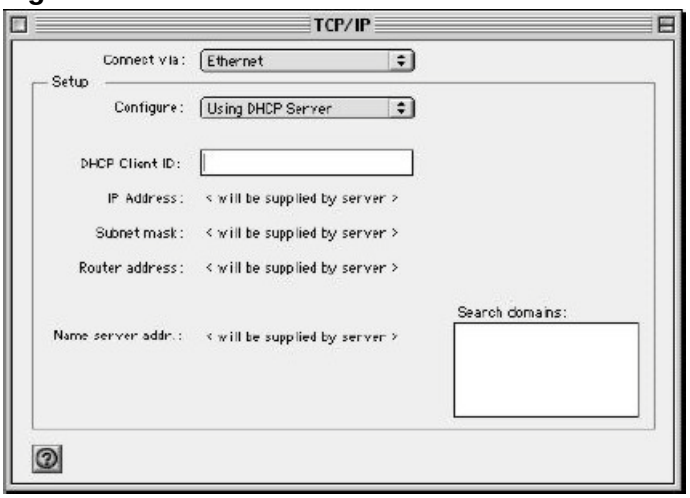
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 140 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 141 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your router and restart your computer (if prompted).

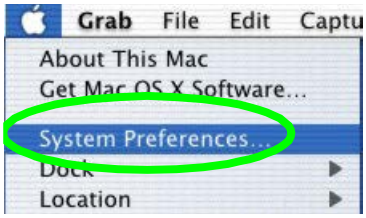
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 142 Macintosh OS X: Apple Menu

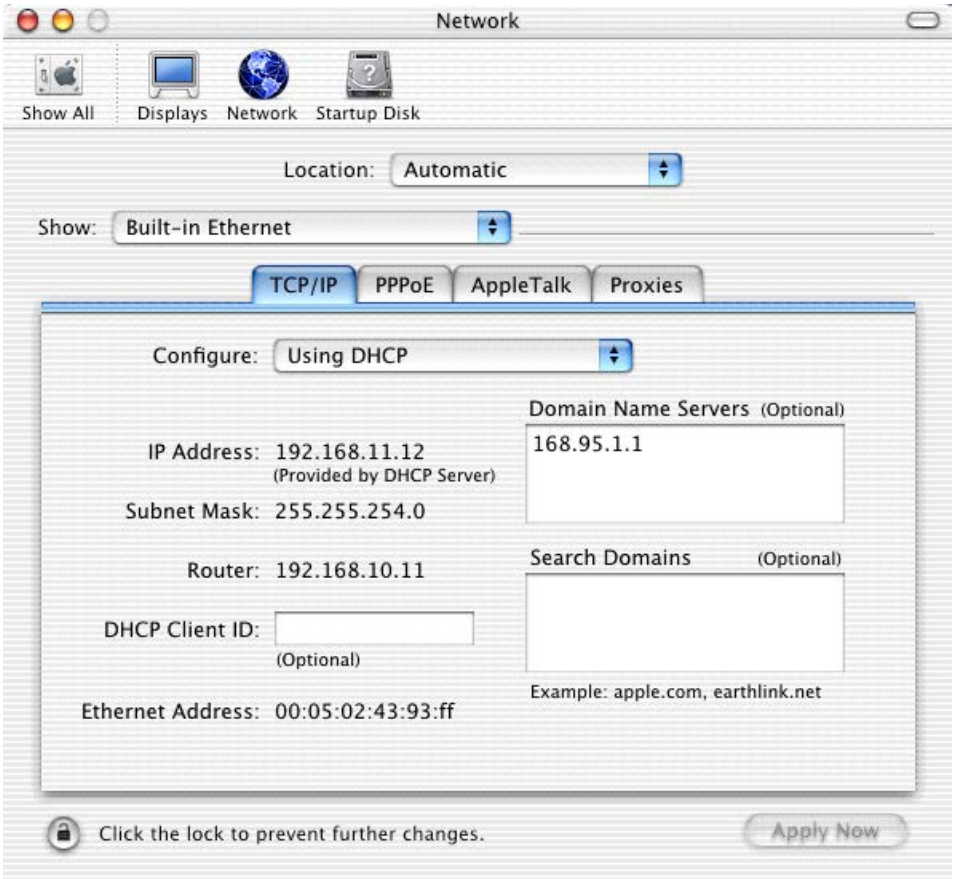


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 143 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your router and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

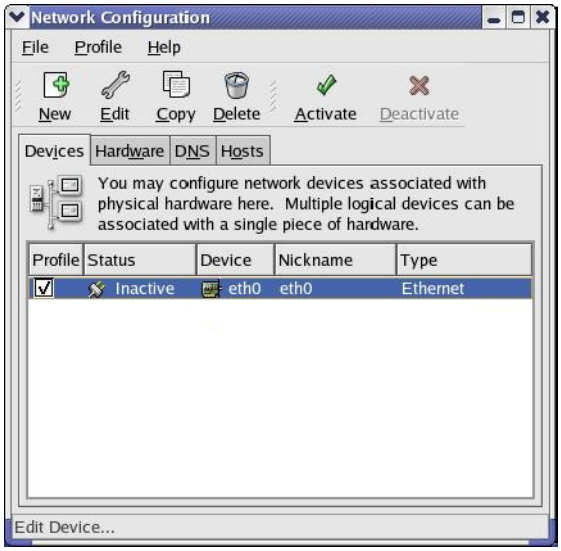
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1. Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 144 Red Hat 9.0: KDE: Network Configuration: Devices



2. Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

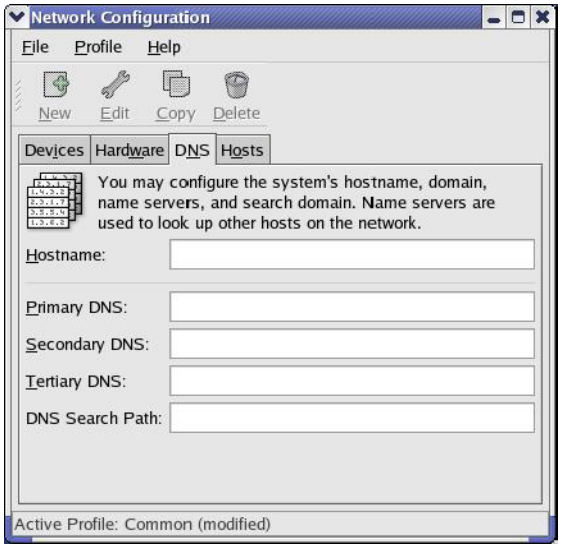
Figure 145 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

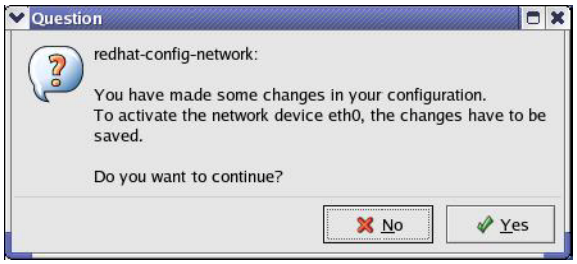
Figure 146 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 147 Red Hat 9.0: KDE: Network Configuration: Activate


Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the BOOTPROTO= field. The following figure shows an example.

Figure 148 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.10.10 and the subnet mask is 255.255.255.0.

Figure 149 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.10.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 150 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 151 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

34.1.2 Verifying Settings

Enter ifconfig in a terminal screen to check your TCP/IP properties.

Figure 152 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

Appendix D

Wireless LANs

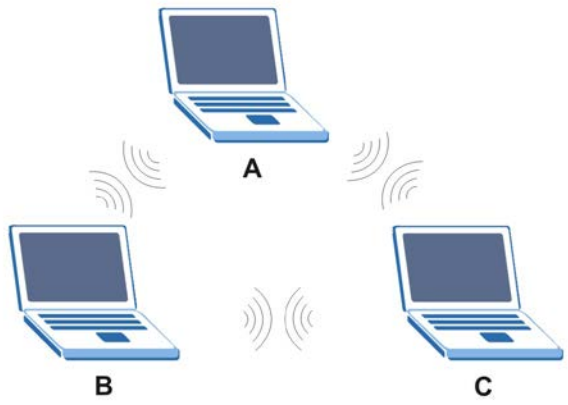
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 153 Peer-to-Peer Communication in an Ad-hoc Network

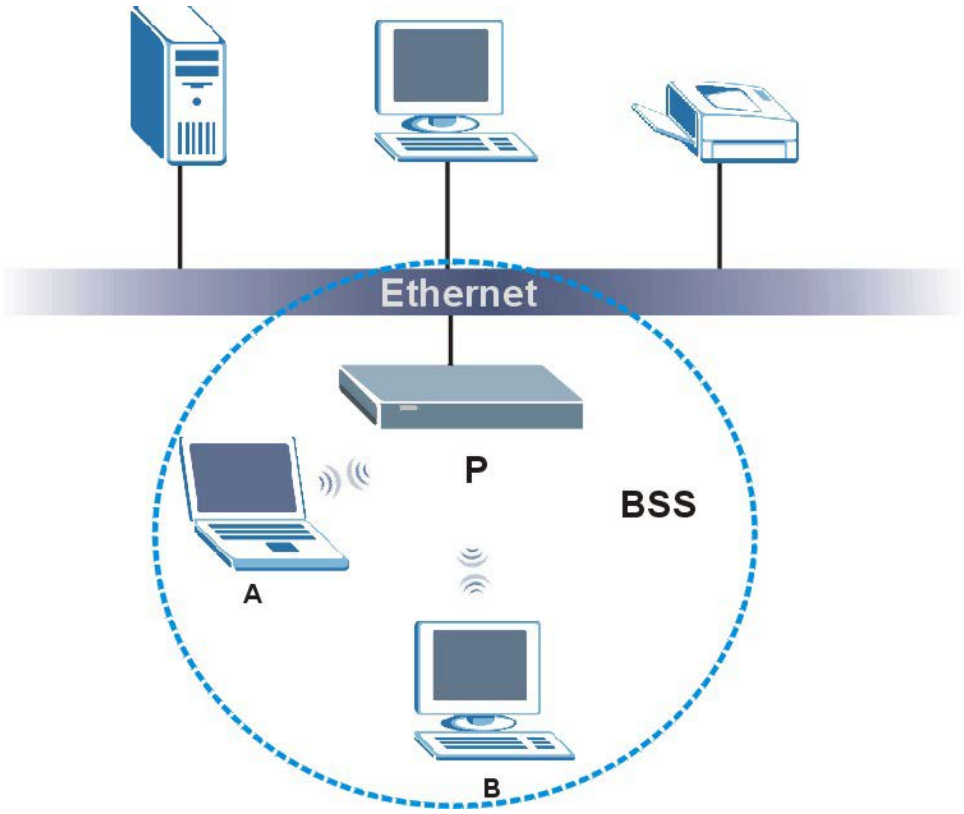


BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 154 Basic Service Set



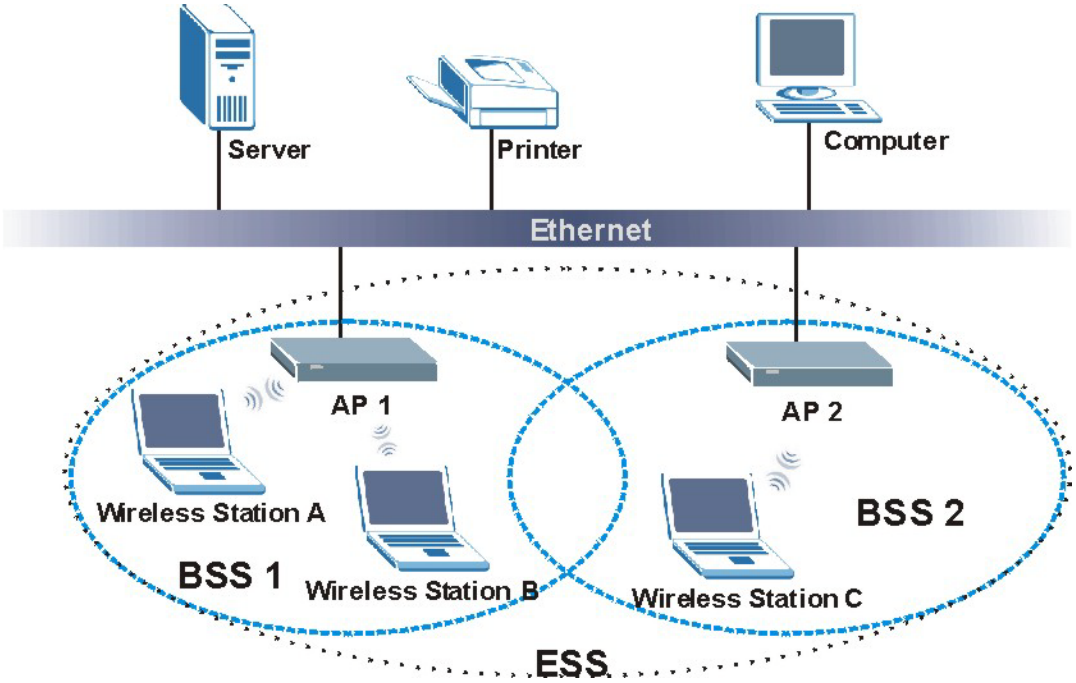
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 155 Infrastructure WLAN



Channel

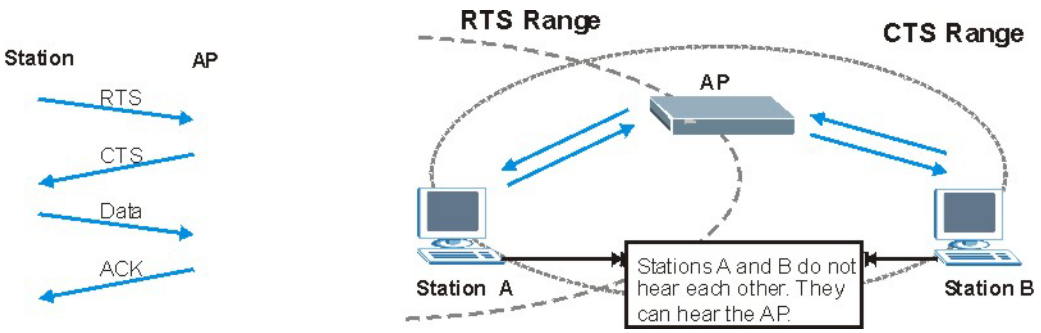
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is, they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 156 RTS/CTS



When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 84 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

  Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with dynamic WEP key exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 85 Comparison of EAP Authentication Types

	EAP-MD5	**EAP-TLS**	**EAP-TTLS**	**PEAP**	**LEAP**
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password,

instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2 -PSK (WPA2 -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

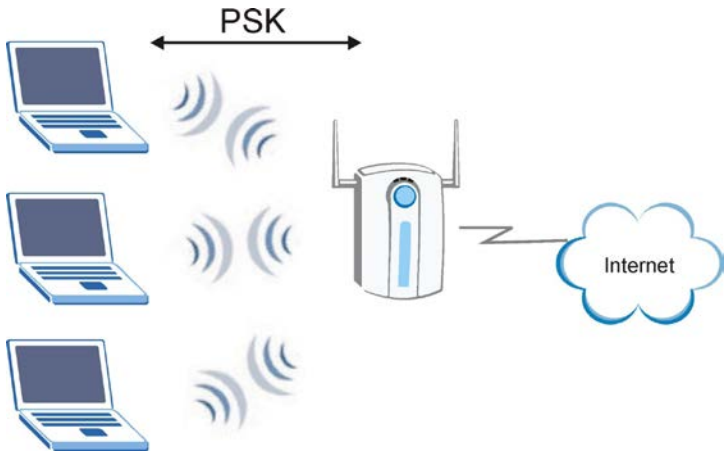
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 157 WPA(2)-PSK Authentication



WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 86 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA-Enterprise	TKIP	No	Enable
WPA-Personal	TKIP	Yes	Enable
WPA2-Enterprise	AES	No	Enable
WPA2-Personal	AES	Yes	Enable

Appendix E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 87 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some

			servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example http://us.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.

IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.

RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Appendix F

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1. this device may not cause interference and
2. this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Viewing Certifications

1. Go to http://us.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of

ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Battery warranty: 1 year

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

GPL-OSS Software Notice

In our continuing effort to disclose important and useful information with regards to our products, we would like to inform you that certain products you received from ZyXEL Communications Inc. may contain in part some free software (In accordance with this free software, it is licensed in a way that ensures your freedom to run, copy, distribute, study, change and improve the software.).

Also, certain ZyXEL products include software code developed by third parties, including software code subject to the GNU General Public License ("GPL")

Please refer to the following URLs to get more information:

http://us.zyxel.com/opensource

or

http://us.zyxel.com/Support/GPL-OSS/

Appendix G

Open Source Licenses

End-User License Agreement for “MWR222”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL’S PRODUCTS MAY CONTAIN–IN PART-SOME THIRD PARTY’S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY’S LICENSES (“OPEN-SOURCED COMPONENTS”). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any

rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL

NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (freesoftware@zyxel.com), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

Open-Sourced Components

3RD PARTY SOFTWARE	VERSION	FROM (SOURCE)	LICENSE
Linux Kernel 2.6.21.x	2.6.21	http://www.kernel.org/	GPL 2.0
Busybox 1.12.1	1.12.1	http://www.busybox.net/	GPL 2.0
Dnsmasq 2.40	2.4.0	http://www.thekelleys.org.uk/dnsmasq/doc.html	GPL 2.0
Goahead 2.1.8	2.1.8	http://www.goahead.com/products/webserver/download.aspx	GPL 2.0
Igmpproxy 0.1 beta2	0.1 beta2	http://sourceforge.net/projects/igmpproxy/	GPL 2.0
Inadyn 1.96	1.96	http://www.dyndns.com/support/clients/unix.html or http://inadyn.sourceforge.net/	GPL 2.0
Iproute2-2.6.24-rc7	2.6.24	http://www.linuxfoundation.org/en/Net:Iproute2 or http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2	GPL 2.0
Rp-pppoe 3.8	3.8	http://www.roaringpenguin.com/products/pppoe	GPL 2.0
Iptables 1.4.0rc1	1.4.0rc1	http://www.netfilter.org/downloads.html	GPL 2.0
Updatedd 2.5	2.5	http://mirror.its.uidaho.edu/pub/savannah/updatedd/	GPL 2.0
Linux-igd 1	1	http://sourceforge.net/projects/linux-igd/	GPL 2.0
Lldt 1.2	1.2	http://www.microsoft.com/whdc/connect/rally/rallykit.mspx	GPL 2.0

Ntpclient 2000 345	2000 345	http://doolittle.icarus.com/ntpclient/	GPL 2.0
Wireless_tools 29	Wireless_tools 29	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html	GPL 2.0
Bridge-utils 1.1	1.1	http://www.linuxfoundation.org/en/Net:Bridge	GPL 2.0
Pptp-client 1.7.1	1.7.1	http://pptpclient.sourceforge.net/	GPL 2.0
Ppp 2.4.2	2.4.2	http://ppp.samba.org/ppp/download.html	GPL 2.0
Rp-12tp 0.4	0.4	http://sourceforge.net/projects/rp-l2tp/	GPL 2.0
Wpa_supplicant 0.5.7	0.5.7	http://hostap.epitest.fi/wpa_supplicant/	GPL 2.0
Zebra-0.95a _ripd	0.95a	http://www.zebra.org/	GPL 2.0
Gcc 3.4.2	3.4.2	http://gcc.gnu.org/	GPL 2.0
Uboot 1.1.3	1.1.3	http://sourceforge.net/projects/u-boot/	GPL 2.0
Mtd-utils 1.0.0	1.0.0	ftp://ftp.infradead.org/pub/mtd-utils/ or http://www.linux-mtd.infradead.org/index.html	GPL 2.0
Uclibc 0.9.28	0.9.28	http://www.uclibc.org/	LGPL 2.1
Uclibc++ 0.2.2	0.2.2	http://cxx.uclibc.org/index.html	LGPL 2.1
Libupnp 1.3.1	1.3.1	http://pupnp.sourceforge.net/	BSD
Zlib 1.1.4	1.1.4	http://www.zlib.org or http://sourceforge.net/project/showfiles.php?group_id=5624&package_id=14274&release_id=79109	Zlib
rt2860apd	rt2860	http://www.ralinktech.com/ or http://rt2x00.serialmonkey.com/wiki/index.php/Main_Page	GPL 2.0
comgt-0.32	0.32	http://sourceforge.net/projects/comgt/	GPL 2.0
curl-7.19.7	7.19.7	http://curl.haxx.se/	MIT/X
ethtool	6	http://sourceforge.net/projects/gkernel/files/ethtool/	GPL 2.0
buildroot-gcc342	buildroot-gcc342	http://buildroot.uclibc.org/	GPL 2.0
hso-1.6	1.6	http://www.pharscape.org/forum/index.php?action=dlattach;topic=544.0;attach=3	GPL 2.0
inadyn.source.v1.99	1.99	http://www.inatech.eu/inadyn https://www.opendns.com/support/ddns_files/inadyn.source.v1.99.zip	GPL 2.0
ldso	0.9.28	http://www.uclibc.org/	LGPL 2.1
libcrypt	0.9.28	http://www.uclibc.org/	LGPL 2.1
libintl	0.9.28	http://www.uclibc.org/	LGPL 2.1

libm	0.9.28	http://www.uclibc.org/	LGPL 2.1
libnsl	0.9.28	http://www.uclibc.org/	LGPL 2.1
libnvram	0.9.28	http://www.uclibc.org/	LGPL 2.1
libpthread	0.9.28	http://www.uclibc.org/	LGPL 2.1
libresolv	0.9.28	http://www.uclibc.org/	LGPL 2.1
libusb-0.1.12	0.1.12	http://www.libusb.org/	LGPL 2.1
libusb-1.0.0	1.0.0	http://www.libusb.org/	LGPL 2.1
libutil	0.9.28	http://www.uclibc.org/	LGPL 2.1
lsusb	1.0.0	http://www.libusb.org/	LGPL 2.1
lzma-4.32.0beta5	4.32beta5	http://sourceforge.net/projects/sevenzip/files/LZMA%20SDK/	LGPL 2.1
mkimage	mkimage	http://packages.debian.org/sid/uboot-mkimage	GPL 2.0
mksquash_lzma-3.2	lzma sdk 4.43 squashfs 3.2-r2	http://sourceforge.net/projects/sevenzip/files/LZMA%20SDK/ http://squashfs.sourceforge.net/	LGPL 2.1
lzma sdk 4.43	4.43	http://sourceforge.net/projects/sevenzip/files/LZMA%20SDK/	LGPL 2.1
squashfs 3.2-r2	3.2-r2	http://squashfs.sourceforge.net/	GPL 2.0
mtd_write	mtd_write	http://downloads.openwrt.org/sources/	GPL 2.0
ntp-4.1.2	4.1.2	http://www.eecis.udel.edu/~ntp/ntp_spool/ntp4/ntp-4.1/	NTP
ntpclient	2003_194	http://doolittle.icarus.com/ntpclient/	GPL 2.0
openssl-0.9.8e	0.9.8e	http://www.openssl.org	BSD
pciutils-3.0.0	3.0.0	http://www.kernel.org/pub/software/utils/pciutils	GPL 2.0
pkg-config	0.23	http://pkg-config.freedesktop.org	GPL 2.0
radvd-1.0	1.0	http://www.litech.org/radvd/	RADVD
sdparm-1.02	1.02	http://sg.danny.cz/sg/sdparm.html	SNMPD
snmpd	snmpd	http://www.net-snmp.org/	BSD
usb-modeswitch-1.1.0	1.1.0	http://www.draisberghof.de/usb_modeswitch/	GPL 2.0
wsc_upnp	0.1.1	http://www.ralinktech.com/ or http://rt2x00.serialmonkey.com/wiki/index.php/Main_Page	Ralink and Intel
Sprint4GDeveloperPack	1.1	https://developer.sprint.com/getDocument.do?docId=101032	GPL 2.0 & BSD

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Linux Kernel 2.6.21.x, Busybox 1.12.1, Dnsmasq 2.40, Goahead 2.1.8, Igmpproxy 0.1 beta2, Inadyn 1.96, Iproute2 2.6.24, Rp-pppoe 3.8, Iptables 1.4.0rc1, Updatedd 2.5, Linux-igd 1, Lldt 1.2, Ntpclient 2000 345, Wireless_tools 29, Bridge-utils 1.1, Pptp-client 1.7.1, Ppp 2.4.2, Rp-12tp 0.4, Wpa_supplicant 0.5.7, Zebra-0.95a _ripd, Gcc 3.4.2, Uboot 1.1.3 and Mtd-utils 1.0.0, rt2860apd, comgt-0.32, ethtool, buildroot-gcc342, hso-1.6, inadyn.source.v1.99, mkimage, squashfs 3.2-r2, mtd_write, ntpclient, pciutils-3.0.0, pkg-config, usb-modeswitch-1.1.0 under the GPL License.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute

copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such

modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b

above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of

any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF

THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Uclibc 0.9.28, Uclibc++ 0.2.2, ldso, libcrypt, libintl, libm, libnsl, libpthread, libresolv, libusb-0.1.12, libusb-1.0.0, libnvram, libutil, lsusb, lzma-4.32.0beta5, mksquash_lzma-3.2 under the LGPL License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries.

However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of

running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this

License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice

for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes Libupnp 1.3.1, openssl-0.9.8e, snmpd under the BSD License.

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Zlib 1.1.4 under the Zlib License.

Zlib License

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.2, October 3rd, 2004

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

ZLIB is third party library and has its own license.

files under src/acdk/vfile/zlib are published under following Copyright and license:

zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.3, July 9th, 1998

Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

This Product includes curl-7.19.7 under the Curl MIT/X License.

Curl License

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2010, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose

with or without fee is hereby granted, provided that the above copyright

notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN

NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,

DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR

OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE

OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not

be used in advertising or otherwise to promote the sale, use or other dealings

in this Software without prior written authorization of the copyright holder.

This Product includes libcrypt, libintl, libnsl, libpthread, libresolv, libutil under the GNU Library General Public License, which has been succeeded by the GNU Lesser General Public License

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is

numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will

individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

* a) The modified work must itself be a software library.

* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable

is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions

files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS

WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or

modify it under the terms of the GNU Library General Public

License as published by the Free Software Foundation; either

version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU

Library General Public License for more details.

You should have received a copy of the GNU Library General Public

License along with this library; if not, write to the

Free Software Foundation, Inc., 51 Franklin St, Fifth Floor,

Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in

the library `Frob' (a library for tweaking knobs) written

by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

This Product includes libm under the following License.

Sun Microsystems, Inc.

The routines included in this math library are derived from the

math library for Apple's MacOS X/Darwin math library, which was
itself swiped from FreeBSD. The original copyright information
is as follows:

> Copyright (C) 1993 by Sun Microsystems, Inc. All rights reserved.
>
> Developed at SunPro, a Sun Microsystems, Inc. business.
> Permission to use, copy, modify, and distribute this
> software is freely granted, provided that this notice
> is preserved.

It has been ported to work with uClibc and generally behave
by Erik Andersen <andersen@codepoet.org>
22 May, 2001

This Product includes mksquash_lzma-3.2 under the following License.

mksquash_lzma License

```
/*
 * Copyright (C) 2006 Junjiro Okajima
 * Copyright (C) 2006 Tomas Matejicek, slax.org
 *
 * LICENSE follows the described one in lzma.
 */
/*
 * Copyright (C) 2006 Junjiro Okajima
```

```
 * Copyright (C) 2006 Tomas Matejicek, slax.org
 *
 * LICENSE must follow the one in squashfs.
 */
```

This Product includes radvd-1.0 under the radvd License.

radvd License

The author(s) grant permission for redistribution and use in source and

binary forms, with or without modification, of the software and documentation

provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled

as not being for redistribution (check the version message and/or README),

you are not permitted to redistribute that version of the software in any

way or form.

1. All terms of all other applicable copyrights and licenses must be

followed.

2. Redistributions of source code must retain the authors' copyright

notice(s), this list of conditions, and the following disclaimer.

3. Redistributions in binary form must reproduce the authors' copyright

notice(s), this list of conditions, and the following disclaimer in the

documentation and/or other materials provided with the distribution.

4. All advertising materials mentioning features or use of this software

must display the following acknowledgement with the name(s) of the authors as specified in the copyright notice(s) substituted where indicated:

This product includes software developed by the authors which are mentioned at the start of the source files and other contributors.

5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS ``AS IS'' AND ANY

EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON

ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS

SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes wsc_upnp under the Ralink and Intel License.

wsc_upnp License

//

//

// Copyright (c) 2000-2003 Ralink Corporation

// All rights reserved.

//

// Redistribution and use in source and binary forms, with or without

// modification, are permitted provided that the following conditions are met:

//

// * Redistributions of source code must retain the above copyright notice,

// this list of conditions and the following disclaimer.

// * Redistributions in binary form must reproduce the above copyright notice,

// this list of conditions and the following disclaimer in the documentation

// and/or other materials provided with the distribution.

// * Neither name of Intel Corporation nor the names of its contributors

// may be used to endorse or promote products derived from this software

// without specific prior written permission.

//

// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS

// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR

// A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR

// CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

// EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

// PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR

// PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY

// OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

// NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS

// SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

//

//

//

//

// Copyright (c) 2000-2003 Intel Corporation

// All rights reserved.

//

// Redistribution and use in source and binary forms, with or without

// modification, are permitted provided that the following conditions are met:

//

// * Redistributions of source code must retain the above copyright notice,

// this list of conditions and the following disclaimer.

// * Redistributions in binary form must reproduce the above copyright notice,

// this list of conditions and the following disclaimer in the documentation

// and/or other materials provided with the distribution.

// * Neither name of Intel Corporation nor the names of its contributors

// may be used to endorse or promote products derived from this software

// without specific prior written permission.

//

// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS

// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR

// A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR

// CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

// EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

// PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR

// PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY

// OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

// NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS

// SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

//

//

This Product includes snmpd under the following snmpd License.

snmpd License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been

based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity

pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered

trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,

  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Sdparm-1.02 under the following Sdparm-1.02 License.

Sdparm-1.02 License

Copyright (c) 2005-2006 Douglas Gilbert.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products

derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Mksquash_lzma-3.2 under the following License.

Mksquash_lzma-3.2 License

Copyright (C) 2006, 2007 Junjiro Okajima

Copyright (C) 2006, 2007 Tomas Matejicek, slax.org

#

LICENSE follows the described ones in lzma and squashfs.”

http://www.squashfs-lzma.org/

(lzma443)

www.7-zip.org

“LZMA SDK Copyright (C) 1999-2006 Igor Pavlov

LICENSE

LZMA SDK is available under any of the following licenses:

1) GNU Lesser General Public License (GNU LGPL)

2) Common Public License (CPL)

3) Simplified license for unmodified code (read SPECIAL EXCEPTION)

4) Proprietary license

It means that you can select one of these four options and follow rules of that license.

1,2) GNU LGPL and CPL licenses are pretty similar and both these

licenses are classified as

- "Free software licenses" at http://www.gnu.org/

- "OSI-approved" at http://www.opensource.org/

3) SPECIAL EXCEPTION

Igor Pavlov, as the author of this code, expressly permits you

to statically or dynamically link your code (or bind by name)

to the files from LZMA SDK without subjecting your linked

code to the terms of the CPL or GNU LGPL.

Any modifications or additions to files from LZMA SDK, however,

are subject to the GNU LGPL or CPL terms.

SPECIAL EXCEPTION allows you to use LZMA SDK in applications with closed code,

while you keep LZMA SDK code unmodified.

SPECIAL EXCEPTION #2: Igor Pavlov, as the author of this code, expressly permits

you to use this code under the same terms and conditions contained in the License

Agreement you have for any previous version of LZMA SDK developed by Igor Pavlov.

SPECIAL EXCEPTION #2 allows owners of proprietary licenses to use latest version

of LZMA SDK as update for previous versions.

SPECIAL EXCEPTION #3: Igor Pavlov, as the author of this code, expressly permits

you to use code of the following files:

BranchTypes.h, LzmaTypes.h, LzmaTest.c, LzmaStateTest.c, LzmaAlone.cpp,

LzmaAlone.cs, LzmaAlone.java

as public domain code.

4) Proprietary license

LZMA SDK also can be available under a proprietary license which

can include:

1) Right to modify code without subjecting modified code to the

terms of the CPL or GNU LGPL

2) Technical support for code

To request such proprietary license or any additional consultations,

send email message from that page:

http://www.7-zip.org/support.html

You should have received a copy of the GNU Lesser General Public

License along with this library; if not, write to the Free Software

Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

You should have received a copy of the Common Public License

along with this library.“

(squshfs3.2-r2)

GPLv2

Copyright 2002-2007 Phillip Lougher <phillip@lougher.org.uk>

http://squashfs.sourceforge.net/

This Product includes libnvram under the following License.

libnvram License

Copyright 2002 Wolfgang Denk, DENX Software Engineering, wd@denx.de.

“/*

* This file is derived from crc32.c from the zlib-1.1.3 distribution

* by Jean-loup Gailly and Mark Adler.

*/

/* crc32.c -- compute the CRC-32 of a data stream

* Copyright (C) 1995-1998 Mark Adler

* For conditions of distribution and use, see copyright notice in zlib.h

*/

This Product includes mkimage under the following License.

mkimage License

NOTE! This copyright does *not* cover the so-called "standalone" applications that use U-Boot services by means of the jump table provided by U-Boot exactly for this purpose - this is merely considered normal use of U-Boot, and does *not* fall under the heading of "derived work". Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code

that it refers to (the U-Boot source code) is copyrighted by me and others who actually wrote it. -- Wolfgang Denk”

(C) Copyright 2000-2003 Wolfgang Denk, DENX Software Engineering, wd@denx.de

/*

* This file is derived from crc32.c from the zlib-1.1.3 distribution

* by Jean-loup Gailly and Mark Adler.

*/

/* crc32.c -- compute the CRC-32 of a data stream

* Copyright (C) 1995-1998 Mark Adler

* For conditions of distribution and use, see copyright notice in zlib.h

*/

http://sourceforge.net/projects/uboot

This Product includes ntp-4.1.2 under the following License.

ntp-4.1.2 License

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
*****************************************************************
*                                                               *
* Copyright (c) University of Delaware 1992-2010                *
*                                                               *
* Permission to use, copy, modify, and distribute this software and
*
* its documentation for any purpose with or without fee is hereby
*
* granted, provided that the above copyright notice appears in all
*
* copies and that both the copyright notice and this permission
*
* notice appear in supporting documentation, and that the name
*
* University of Delaware not be used in advertising or publicity
*
* pertaining to distribution of the software without specific,   *
* written prior permission. The University of Delaware makes no
*
* representations about the suitability this software for any    *
* purpose. It is provided "as is" without express or implied     *
* warranty.                                                     *
*                                                               *
*****************************************************************
```

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller

2. Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices

3. Viraj Bais <vbais@mailman1.intel.com> and Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5

4. Michael Barone <michael,barone@lmco.com> GPSVME fixes

5. Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca>IPv6 support

6. Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option

7. Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.

8. Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver

9. Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support

10. Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)

11. Steve Clift <clift@ml.csiro.au> OMEGA clock driver

12. Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration

13. Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.

14. John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port

15. Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port

16. Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119

17. John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing

18. Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite.

19. Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver

20. Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver

21. Mike Iglesias <iglesias@uci.edu> DEC Alpha port

22. Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port

23. Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul

24. Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or <H.Lambermont@chello.nl> ntpsweep

25. Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)

26. Frank Kardel <kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling

27. William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications

28. Dave Katz <dkatz@cisco.com> RS/6000 AIX port

29. Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver

30. George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port

31. Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication

32. Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305

33. Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance

34. David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG

35. Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port

36. Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility

37. Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port

38. Kamal A Mostafa <kamal@whence.com> SCO OpenServer port

39. Derek Mulcahy <derek@toybox.demon.co.uk> and Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver

40. Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance

41. Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling

42. Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port

43. Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo

44. Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules

45. Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory

46. Ray Schnitzler <schnitz@unipress.com> Unixware1 port

47. Michael Shields <shields@tembel.org> USNO clock driver

48. Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver

49. Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)

50. Kenneth Stone <ken@sdd.hp.com> HP-UX port

51. Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support

52. Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver

53. Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver

54. Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD